Data object management method to comply with predetermined conditions for use, e.g for electronic delivery of books etc - storing predetermined set of conditions e.g time limit for use of data object in memory with data object, for enabling or disabling use of object by user

Patent Assignee: BENSON G (BENS-I); KNAUFT C L (KNAU-I); MACROVISION CORP (MACR-N); MEDIADNA INC (MEDI-N); URICH G H (URIC-I)
Inventor: BENSON G; KNAUFT C; KNAUFT C L; URICH G; URICH G H; URICH G Q ; URICH H

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
JP 10513289	W	19981215	JP 1996523476	A	19960201	199909	E

Abstract
The method for managing a data object so as to comply with predetermined conditions of use involves storing the data object in memory, where it is accessible by the object provider's processor, and creating a set of control data, defining usages of the data object which comply with the predetermined conditions, e.g geographical area of use, claim to royalty payment etc, for the stored data object, to control usage of the data object.
The data object is concatenated with the user set of control data, encrypted and transferred to the user. When the user wants to use the data object, a special user program checks whether the usage complies with the control data, and if it does, the usage is enabled, otherwise it is disabled.
USE - Managing data object independently of format and structure of object, so as to comply with predetermined conditions for use control and royalty payments, e.g for books, films, video, news, music, software, games etc.
ADVANTAGE - Universally adaptable to owner and user of data object. Enables data object provider to distribute data object while maintaining control of usage of object.

Original Abstract:
The present invention relates to a method and a system for managing a data object so as to comply with predetermined conditions for usage of the data object. To control the usage of the data object, a set of control data, defining usages of the data object which comply with the predetermined conditions, is created for the data object. The data object is concatenated with the user set of control data, encrypted and transferred to the user.When the user wants to use the data object, a special user program checks whether the usage complies with the control data. If so, the usage is enabled. Otherwise it is disabled.

A method and a system for managing a data object so as to comply with predetermined conditions for usage of the data object. To control the usage of the data object, a set of control data, defining uses of the data object, which comply with the predetermined conditions, is created for the data object. The data object is concatenated with the user set of control data, encrypted and transferred to the user. When the user wants to use the data object, a special user program checks whether the usage complies with the control data. If so, the usage is enabled. Otherwise it is disabled.

(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号

特表平10－513289

(43)公表日　平成10年(1998)12月15日

(51)Int.Cl.⁶		識別記号	FI		
Ｇ０６Ｆ	17/60		Ｇ０６Ｆ	15/21	３３０
	9/06	５５０		9/06	５５０Ａ
					５５０Ｚ
	15/00	３３０		15/00	３３０Ｚ
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｄ

審査請求　未請求　予備審査請求　有　（全 57 頁）　最終頁に続く

(21)出願番号　特願平8－523476
(85)(22)出願日　平成８年(1996)２月１日
(85)翻訳文提出日　平成９年(1997)７月31日
(86)国際出願番号　ＰＣＴ／ＳＥ９６／００１１５
(87)国際公開番号　ＷＯ９６／２４０９２
(87)国際公開日　平成８年(1996)８月８日
(31)優先権主張番号　９５００３５５－４
(32)優先日　1995年２月１日
(33)優先権主張国　スウェーデン（ＳＥ）

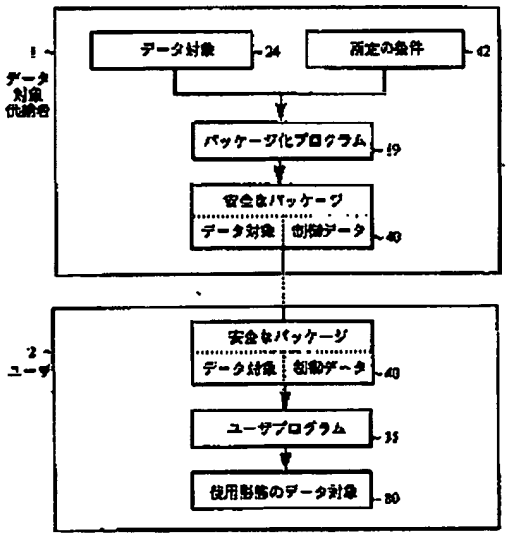
(71)出願人　ベンソン，グレグ
スウェーデン国エス－240　10　ダルビイ，ダルバッカベーゲン　３
(72)発明者　ベンソン，グレグ
スウェーデン国エス－240　10　ダルビイ，ダルバッカベーゲン　３
(72)発明者　ユーリッチ，グレゴリー　エイチ，
スウェーデン国エス－224　65　ルンド，ヴァルホルムスベーゲン　８ビー
(74)代理人　弁理士　浅村　皓　（外３名）

最終頁に続く

(54)【発明の名称】　所定の使用条件を満たすようにデータ対象を管理するための方法およびシステム

(57)【要約】
本発明はデータ対象の所定の使用条件に従うようにデータ対象を管理するための方法およびシステムに関する。データ対象の使用を制御するために、所定の条件に従うデータ対象の使用を定める組の制御データがデータ対象に対して作られる。データ対象はユーザの組の制御データと連結され、暗号化され、ユーザに転送される。ユーザがデータ対象を使用したい時には、使用が制御データに従うかどうか特別なユーザプログラムがチェックする。そうであれば、使用は可能化される。そうでなければ、それは無能化される。

Fig 1



【特許請求の範囲】

1．データ対象の使用のための所定の条件に従うようにデータ対象を管理する方法において、

データ対象をメモリ装置に記憶し、そこでデータ対象がデータ対象供給者のデータプロセッサによりアクセス可能となるようにすること、

上記データプロセッサによって、上記所定の使用条件に基づいてデータ対象のための全体的な組の制御データを作成し、上記全体的な組の制御データが上記所定の条件に従うデータ対象の使用を定める少なくとも1つあるいはそれ以上の使用制御要素からなるようにすること、

上記全体的な組の制御データをメモリ装置に記憶し、そこでそれが上記データプロセッサによってアクセス可能となるようにすること、

全体的な組の制御データをデータ対象のコピーと連結すること、

少なくともデータ対象のコピーと上記1つあるいはそれ以上の使用制御要素を暗号化して、ユーザへの転送のための準備状態にある安全なデータパッケージを作ること、

のステップを具備してなる方法。

2．請求の範囲第1項記載の方法において、暗号化するステップはデータ対象および全体的な組の制御データを暗号化することからなる方法。

3．請求の範囲第1項あるいは第2項記載の方法において、制御データを作るステップは全体の組の制御データを区別して識別する識別子を作ることからなる方法。

4．請求の範囲第1項、第2項あるいは第3項記載の方法において、全体の組の制御データを作るステップは、データ対象の使用が許される前に与えられるセキュリティプロセスを識別するセキュリティ制御要素を作ることからなる方法。

5．請求の範囲の上述の項のうちの任意の1項記載の方法において、全体の組の制御データを作るステップは制御データのフォーマットを識別するフォーマット制御要素を作ることからなる方法。

6．請求の範囲の上述の項のうちの任意の1項記載の方法において、

ユーザによるデータ対象の使用許可のための要求に応じて、上記使用制御要素の少なくとも1つを含む全体の組の制御データの少なくともサブセットからなるユーザの組の制御データを作ること、

上記結合するステップにおいて、全体の組の制御データの代わりにユーザの組の制御データを用いること、

上記暗号化するステップにおいて、全体の組の制御データの上記1つあるいはそれ以上の使用制御要素の代わりにユーザの組の制御データの上記少なくとも1つの使用制御要素を用いること、

ユーザへのデータパッケージの転送を行う前に、データ対象の使用許可の上記要求が承諾されたことをチェックすること、

のステップを更に具備した方法。

7．請求の範囲の上述の項のうちの任意の1項記載の方法において、上記データプロセッサにおいてユーザによる使用許可のための要求を受けること、許可が要求される使用を全体の組の制御データの上記1つあるいはそれ以上の使用制御要素と比較すること、許可が要求される使用が上記少なくとも1つあるいはそれ以上の使用制御要素によって定められる使用に従う場合に許可を承諾すること、のステップを更に具備した方法。

8．請求の範囲第7項記載の方法において、許可を承諾する前に要求された使用許可のための支払いを確実化するステップを更に具備した方法。

9．請求の範囲第6－8項のうちの任意の1項記載の方法において、データ対象は少なくとも2つの構成要素データ対象からなり、ユーザの組の制御データは、ユーザによる上記構成要素データ対象の1つの使用に対する許可の要求に応じて、その構成要素データ対象に対してだけに作られてこの構成要素データ対象のコピーとだけに連結されることを特徴とする方法。

10．請求の範囲第6－9項のうちの任意の1項記載の方法において、データ供給者のデータプロセッサはデータネットワークに接続され、許可の要求は同様このデータネットワークに接続したユーザのデータプロセッサから受けられるようになっており、データパッケージを上記データネットワークを介してユーザ

のデータプロセッサに転送するステップを更に具備した方法。

11. 請求の範囲第6－8項あるいは第10項のうちの任意の1項記載の方法において、データ対象は少なくとも2つの構成要素データ対象を含んだ複合データ対象であり、全体の組の制御データを作るステップは複合データ対象のそれぞれおよび複合データ対象に対するそれぞれの全体の組の制御データを作るステップからなり、ユーザの組の制御データを作るステップは構成要素データ対象のそれぞれおよび複合データ対象に対するそれぞれのユーザの組の制御データを作るステップからなる方法。

12. 請求の範囲の上述の項のうちの任意の1項記載の方法において、ユーザの組の制御データのコピーをデータ対象供給者のプロセッサに記憶するステップを更に具備した方法。

13. 請求の範囲の上述の項のうちの任意の1項記載の記載の方法において、

ユーザのデータプロセッサのデータパッケージを受けること、

メモリ装置にデータパッケージを記憶し、そこでそれがユーザのデータプロセッサによりアクセス可能となるようにすること、

上記1つあるいはそれ以上の使用制御要素を暗号解除すること、

データ対象の使用のためのユーザによる要求に応じて、要求された使用が全体の組の制御データの少なくとも1つの使用制御要素によって規定された使用に従うかどうかをチェックすること、

全体の組の制御データの少なくとも1つの使用制御要素によって規定される使用に従う要求された使用に応じて、データ対象を暗号解除して要求された使用を可能化し、そうでなければそれを無能化すること、

のステップを更に具備した方法。

14. 請求の範囲第6－12項のうちの任意の1項記載の方法において、

ユーザのデータプロセッサのデータパッケージを受けること、

メモリ装置にデータパッケージを記憶し、そこでそれがユーザのデータプロセッサによりアクセス可能となるようにすること、

ユーザの組の制御データの上記少なくとも1つの使用制御要素を暗号解除すること、

データ対象の使用のためのユーザによる要求に応じて、要求された使用がユーザの組の制御データの少なくとも1つの使用制御要素によって規定された使用に従うかどうかをチェックすること、

ユーザの組の制御データの少なくとも1つの使用制御要素によって規定される使用に従う要求された使用に応じて、データ対象を暗号解除して要求された使用を可能化し、そうでなければそれを無能化すること、

のステップを更に具備した方法。

15. 請求の範囲第13項あるいは第14項記載の方法において、データ対象の使用の後に、データ対象および1つあるいはそれ以上の使用制御要素を再連結すること、少なくともデータ対象および1つあるいはそれ以上の使用制御要素を再暗号化すること、このようにして再パッケージ化したデータパッケージをユーザのデータプロセッサのメモリに記憶すること、のステップを更に具備した方法。

16. データ対象の所定の使用条件に従うようにデータ対象のユーザによる使用を制御するための方法において、

データパッケージをメモリ装置に記憶し、そこでそれがユーザのデータプロセッサによりアクセス可能となるようにし、上記データパッケージがデータ対象と制御データからなり、その制御データが所定の条件に従うデータ対象の使用を定める少なくとも1つの使用制御要素からなり、データ対象および上記少なくとも1つの使用制御要素は暗号化されるようにすること、

データ対象の使用に対するユーザによる要求を受けること、

制御データを暗号解除すること、

データ対象の使用のためのユーザによる要求に応じて、要求された使用が制御データの少なくとも1つの使用制御要素によって規定された使用に従うかどうかをチェックすること、

制御データの少なくとも1つの使用制御要素によって規定される使用に従う要求された使用に応じて、データ対象を暗号解除して要求された使用を可能化し、そうでなければそれを無能化すること、

のステップを具備した方法。

17. 請求の範囲第16項記載の方法において、使用制御要素はデータ対象の使用の後に更新されるようにした方法。

18. 請求の範囲第16項あるいは第17項記載の方法において、上記制御データは上記少なくとも1つのユーザ制御要素に従ってユーザがデータ対象を使用することを許可される回数の指示からなり、データ対象の要求された使用は上記回数が1あるいはそれ以上の時にのみ可能化され、上記回数は要求された使用が可能化される時に1だけ減少されるようにした方法。

19. 請求の範囲第16－18項のうちの任意の1項記載の方法において、制御データはセキュリティ制御要素を備え、更に、データ対象の各使用の前にセキュリティ制御要素において定められたセキュリティプロシージャを実行するステップを具備した方法。

20. 請求の範囲第16－19項のうちの任意の1項記載の方法において、要求された使用が少なくとも1つの使用制御要素によって規定された使用に従うかどうかをチェックするステップは、ユーザのデータプロセッサがユーザの組の制御データのセキュリティ制御要素で特定されたセキュリティプロシージャを実行し、そうでなければ使用を無能化することができることをチェックするステップからなるようにした方法。

21. 請求の範囲第16－20項のうちの任意の1項記載の方法において、データ対象の使用の後に、データ対象および1つあるいはそれ以上の使用制御要素を再連結すること、少なくともデータ対象および1つあるいはそれ以上の使用制御要素を再暗号化すること、このようにした再パッケージ化されたデータパッケージをユーザのデータプロセッサのメモリに記憶すること、のステップを更に具備した方法。

22. データ対象の所定の使用条件に従うようにデータ対象を管理するシステムにおいて、

データ対象供給者のデータプロセッサに設けられ、上記所定の使用条件に基づいてデータ対象のための全体の組の制御データを作り、この全体の組の制御データが上記所定の条件に従うデータ対象の使用を定める少なくとも1つあるいはそれ以上の使用制御要素からなるようにする第1の手段と、

上記データプロセッサによりアクセス可能とされ、データ対象と全体の組の制御データを記憶するための記憶手段と、

全体の組の制御データをデータ対象のコピーと連結するための連結手段と、

データ対象のコピーと少なくとも上記1つあるいはそれ以上の使用制御要素を暗号化して、ユーザへの転送のための準備状態にある安全なデータパッケージを作る案等価手段と、

を具備してなるシステム。

23. 請求の範囲第22項記載のシステムにおいて、

上記データプロセッサに設けられ、ユーザによるデータ対象の使用許可の要求に応じて、上記使用制御要素の少なくとも1つからなる全体の組の制御データのサブセットから少なくとも構成されるユーザの組の制御データを作る第2の手段と、

上記データプロセッサに設けられ、データ対象の使用許可のための上記要求がユーザへのデータパッケージの転送を行わせる前に承諾されたことをチェックするチェック手段と、を更に具備したシステム。

24. 請求の範囲第22項あるいは第23項記載のシステムにおいて、全体の組の制御データはユーザによるデータ対象の一層の配布に対する権利を定める制御データ要素を備えたシステム。

25. データ対象の所定の使用条件に従うようにデータ対象のユーザによる使用を制御するためのシステムにおいて、

データ対象と制御データからなり、その制御データが所定の条件に従うデータ対象の使用を定める少なくとも1つの使用制御要素からなるようなデータパッケージを記憶するための記憶手段と、

上記少なくとも1つの使用制御要素およびデータ対象を暗号解除する手段と、

ユーザにより要求された使用が上記少なくとも1つの使用制御要素によって定められる使用に従うかどうかをチェックするためのチェック手段と、

使用が上記少なくとも1つの使用制御要素によって定められた使用に従う時にユーザによって要求された使用を可能化するための可能化手段と、

使用が上記少なくとも1つの使用制御要素によって定められた使用に従わない

時にユーザによって要求された使用を不能化するための不能化手段と、

を具備してなるシステム。

26. 請求の範囲第25項記載のシステムにおいて、データ対象の使用後にデータ対象を再パッケージ化するための手段を更に具備したシステム。

27. データ対象の所定の使用条件に従うようにデータ対象のユーザによる使用を制御するための方法において、

メモリ装置に少なくとも2つのデータパッケージを記憶し、そこでそれらがユーザのデータプロセッサによりアクセス可能となるようにされ、上記データパッケージのそれぞれがデータ対象と、上記所定の使用条件に従うデータ対象の使用を定める少なくとも1つの使用制御要素からなるユーザの組の制御データとからなるようにし、データ対象および上記少なくとも1つの使用制御要素が暗号化されるようにすること、

ユーザの組の制御データの使用制御要素を暗号解除すること、

上記少なくとも2つのデータパッケージの使用制御要素を検査して一致を見い出すこと、

一致が見い出されることに応じて、ユーザの組の制御データにおいて特定化される行為を実行するように上記データプロセッサを用いること、

のステップを具備してなる方法。

28. 請求の範囲第27項記載の方法において、各データパッケージの使用制御要素を更新すること、データ対象の使用の後に、データ対象のそれぞれとその使用制御要素とを再連結すること、連結されたデータ対象のそれぞれとその使用制御要素とを再暗号化すること、これら再パッケージ化したデータ対象をそれらの創造者に転送すること、のステップを更に具備した方法。

【発明の詳細な説明】

所定の使用条件を満たすようにデータ対象を管理するための方法およびシステム

技術分野

本発明はデータ処理に関し、より詳細には、所定の使用条件を満たすようにデータ対象を管理するための方法およびシステムに関する。

背景

最近、万能接続可能性（ｕｎｉｖｅｒｓａｌ　ｃｏｎｎｅｃｔｉｖｉｔｙ）の問題に関する多くのものが執筆されている。データハイウェイの典型的な予測は、電気通信サービスと需要者に対して広範囲のインタラクティブ・オンラインサービスとを提供する地域ネットワークを相互接続する長距離、高速データキャリアにある。多くのものが既に実用化しているが、他のものは開発中であるか、あるいは試験中である。実際上、データハイウェイが構築中であっても、それは限られたトラフィックに対しては現在公開状態である。オンラインサービスは日々出現しているが、ビデオ　オンデマンドサービスは現在試験中である。

社会が利益を受ける潜在性は広大である。需要者にとって利用可能な情報の範囲は、情報の分配および情報へのアクセスのためのエントリに対する伝統的な障壁が劇的に低下しているために真に世界的規模になる。これは、より多種化しかつ特殊化した情報がそのように使用される大きなベンダからの一般的なソースと同様に便利に利用可能とされることを意味する。最終の結果は、組織および個人が幾分これまでにただ想像していただけの態様で権能が与えられる。

しかしながら、完全に機能するデータハイウェイはそれが与える実際のサービスと同じ程価値があるにすぎない。データ対象（例えば、本、フィルム、ビデオ、ニュース、音楽、ソフトウェア、ゲーム等）の供給を含むデータハイウェイに対して想定されるサービスはこのような対象の有効性により制限されることになろうし、現在制限されている。ライブラリおよび教育サービスも同様影響される。所有者が自己のデータを提供する前に、ローヤリティの支払いおよび著作権侵害行為からの保護を確保する必要がある。

暗号化はコピー保護を与える何等かの解決法のキー要素である。しかしながら

、暗号化そのものは十分ではない。伝送および記憶の間に、データ対象は暗号化によって保護されるであろうが、誰かが内容を暗号解読するキーを与えられたら、その人物はそれに対する非制限的支配を持つことになる。デジタル域はデータ対象を品位の損失無く無制限の量再生できるようにするため、各対象は非制限的な使用ならびに無許可の再生および再販売から保護される必要がある。

この保護の問題は各特定のデータフォーマットに対する個別の解決法によっては解決されてはならず、これはその時進歩が実際ゆっくりしているためである。産業界での標準化の効果を考慮することが重要である。ＶＨＳ、ＣＤおよびＤＡＴフォーマットならびにＩＢＭのＰＣ互換性規準がそれらそれぞれの産業界でどのようにして成長したかを考慮されたい。しかしながら、任意の形式の規格が存在していれば、データ提供者およびデータ使用者の両者の必要性にとっての万能の適応性をその規格が与えなければならない。

データ対象の所有者は、どのように、いつ、どこで、誰により自己の財産が使用されるかについての永久的な安全管理を欲するかもしれない。更にまた、その所有者は特定の対象の価値に依存して種々の形式のユーザおよび種々の形式のセキュリティに対する保証の種々の基準を定めることを欲するかもしれない。その所有者によって定められた基準はデータサービスおよびネットワーキングによって可能化される自動化動作を支配することになる。使用者は、また、各成分対象を支配する種々の基準と共に成分対象を販売することを欲するかもしれない。従って、変わり易く拡張性のある管理を実行できることが必要となる。

その所有者の役割に関連するユーザはデータ対象を便利な態様で検索できかつ購入できうることを欲する。望むならば、ユーザは購入した対象を結合あるいは編集する（すなわち、プレゼンテーションを作るため）ことができなければならない。更にまた、ユーザは子供を不適当な材料から保護することを欲するかもしれない。完全な解決法はこれらの要求をその上可能にしなければならない。

必要なものはデータ対象の所有者およびユーザの利益を保護しつつ、データ対象の交換および使用を管理するための万能可適応システムおよび方法である。

従来技術

ソフトコピー本をコピーする時にローヤリティの支払いを強要するための方法は欧州特許出願ＥＰ０　５６７　８００号に記載されている。この方法は特殊なタグを有するローヤリティ支払い要素を含む構造化文書のフォーマットされたテキストストリームを保護する。このフォーマットされたテキストストリームがユーザのデータプロセッサに入力されると、テキストストリームがローヤリティ支払い要素を識別するように検索され、フラッグがデータプロセッサのメモリに記憶される。ユーザが例えば文書を印刷することを要求すると、データプロセッサは第２のデータプロセッサからこの動作のための許可を要求する。この第２のデータプロセッサはローヤリティ支払い要素において指示された額をユーザに請求し、次いで許可を第１のデータプロセッサに送る。

この方法の１つの重大な制限はそれが単に構造化された文書に対して与えられるに過ぎないことである。上述の欧州特許出願の記載は、ＳＧＭＬに従った形式の定義に従って準備された文書として構造化文書を規定する。換言すれば、それはＳＧＭＬに従っていない文書には適用され得ず、他のどの形式のデータ対象にも適用され得ない。

更にまた、この方法は可変で拡張性のある管理を与えない。誰もがＣＤ、フロッピーディスク等でソフトコピー本を購入することができ、同一のローヤリティの額が同一タイトルの全てのソフトコピー本のローヤリティ支払い要素において指示される。

従って、ＥＰ０　５６７　８００号に記載される方法はデータ対象の万能的可適応保護のための上述した要求を満たさない。

発明の概要

従って、使用管理およびローヤリティ支払いのための所定の条件に従うようにデータ対象のフォーマットおよび構造に無関係の態様でデータ対象を管理するための方法およびデータ処理システムを与えることが本発明の第１の目的である。

データ対象の所有者およびユーザの両者の要請に対して万能的に可適応性である上記のような方法およびシステムを与えることが本発明の他の目的である。

本発明の更に他の目的は、データ対象の提供者が、データ対象のユーザの管理を維持する状態でデータ対象を配布することができるようにする上述した方法お

よびシステムを与えることである。

本発明の更に他の目的は、データ対象の供給者が自己のデータ対象のためのセキュリティのレベルを融通性ある態様で選択することができるようにする方法およびシステムを与えることである。

本発明の更に他の目的はデータ対象のための監査証跡を確立することを可能とする上記のような方法およびシステムを与えることである。

本発明の更に他の目的はデータ対象を安全な態様で売買することを可能とする上記のような方法およびシステムを提供することである。

上記の目的は請求の範囲第1項、16項、22項、25項および27項の特徴を有する方法およびシステムによって達成される。

本発明の特定の実施例は請求の範囲の従属項に記載されている。

より詳細には、データ対象の提供者、例えば、データ対象の所有者あるいはその代理人（ブローカ）はメモリ装置、例えば大規模記憶装置にデータ対象を記憶し、そこでそれはデータ提供者のデータプロセッサによってアクセス可能となる。データ対象はデジタルデータ、アナログデータあるいはアナログおよびデジタルの混成の組合せからなることができる。

データ対象の使用のための所定の条件に基づく全体の組の制御データが作られてデータ対象と同じメモリ装置かあるいはそれがデータ供給者のデータプロセッサによってアクセス可能となるような他のメモリ装置に記憶される。この所定の使用条件はデータ対象の所有者、ブローカあるいは他の任意のものによって定められてもよい。それらは種々のデータ対象間で相違してもよい。

全体の組の制御データは少なくとも1つあるいはそれ以上の使用制御要素を具備しており、これら要素は使用条件に従ったデータ対象の使用を定める。これらの使用は、例えば使用の種類、使用のための時間制限、使用の地理的区域、データ対象のハードコピーを作ったりそれを見るといった許可された動作、および／またはローヤリティ支払いに対するクレームを含んでもよい。全体の組の制御データは使用制御要素以外の他の種類の制御要素からなってもよい。好適実施例において、全体の組の制御データはデータ対象の使用の前に行われなければならないセキュリティプロシージャを定めるセキュリティ制御要素を具備している。ま

た、それは全体の組の制御データを一意に識別する識別子を具備している。

全体の組の制御データはデータ対象のコピーと連結されている。従って、制御データはデータ対象に属せず、その外部に存在し、これは制御データをデータ対象のフォーマットおよびその種類から独立となるようにし、かつ使用管理がデータ対象と独立となることができるようにする。

少なくとも使用制御要素およびデータ対象は暗号化されて、ユーザが使用制御を行いかつデータ対象を暗号解読するユーザプログラム無しではデータ対象を使用できないようにする。別態様として、全体の組の制御データおよびデータ対象のコピーが暗号化されてもよい。

ユーザは、データネットワークを介したあるいは任意の他の適切な態様でデータ供給者のデータプロセッサに属するデータ対象の使用のための認可を要請することができる。この許可は支払いを必要としたり、あるいは必要としなくともよい。使用許可の要請を受けると、ユーザの組の制御データがデータ提供者のプロセッサによって作られる。ユーザの組の制御データは全体の組の制御データ、あるいはそのサブセット（実際のユーザに関連した少なくとも1つの上記制御要素を含む）からなる。また、それは、典型的に、この組の制御データを一意に識別する新たな識別子を含んでいる。もし関連するならば、ユーザの組の制御データは、また、許可された使用の数の指示を備えている。1種類以上の使用が許可されるならば、各種類の使用の数が特定されてもよい。最後に、使用者の組の制御データがデータ対象のコピーと結合され、少なくとも使用制御要素およびデータ対象のコピーがユーザへの転送の準備のため安全なデータパッケージを作るように暗号化される。

データパッケージがユーザに転送される前に、使用許可の要請が承諾されていることが確認されなければならない。好ましくは、ユーザの組の制御データが作られる前にチェックが行われる。しかしながら、それは、また、ユーザの制御データの作成と並列にあるいはその後に行われることもできる。後者の場合に、ユーザによって要請された使用の数が暫定的に許可され、ユーザの組に含まれるが、要請が拒絶されると、ユーザの組は取り消されるか、あるいは変更される。

データパッケージは電子的手段によってユーザに転送されても、あるいは大規

様記憶媒体に記憶されてメールによってあるいは任意の好ましい輸送手段によってユーザに転送されてもよい。

一旦データ対象が上述の態様でパッケージ化されたら、それは、使用制御を内蔵したユーザプログラムおよびデータパッケージを暗号解読する手段によってのみアドレスされることができる。ユーザプログラムは制御データにおいて受け入れられ得るものとして定められた使用を行わせるに過ぎない。更にまた、制御データがセキュリティ制御要素を具備しているならば、ここに規定されているセキュリティプロシージャに従わなければならない。一実施例において、使用制御は次のようにして行われることができる。ユーザがデータ対象を使うことを決定すれば、ユーザプログラムはこの行為が許可されるかどうかを調べるために制御データをチェックする。より詳細には、それは、この種類の許可された使用の数が1つあるいはそれ以上であるかをチェックする。そうであれば、その行為は可能となり、許可された使用の数は1だけ減少される。そうでなければ、ユーザプログラムによってその行為は中断され、ユーザにはその行為を行うための権利を購入する機会が与えられるか、あるいは禁止されることができる。

使用後に、ユーザプログラムは前にパッケージされたと同じ態様でデータ対象をパッケージ解除する。

データ対象がユーザあるいはブローカによって再配布される時には、新たな制御要素が制御データに加えられ、元のユーザ／ブローカと新規なユーザ／ブローカとの間の関係を反映するようにされる。この態様で、データ対象のための監査証跡が作られることができる。

本発明の他の特徴によれば、少なくとも2つのデータパッケージがユーザのデータプロセッサに記憶され、これは一致を見い出すためにデータパッケージの使用制御要素を検査する。一致が見い出されたら、ユーザのデータプロセッサはユーザの組の制御データにおいて特定された行為を行う。この方法はデータ対象を売買するために使用され得る。

図面の簡単な説明

第1図は本発明による全体のデータの流れを示す流れ図である。

第2図はデータ対象の供給者のデータプロセッサのシステムブロック図である

。

第3図は本発明によるデータパッケージ化プログラムの別のモジュールを示すブロック図である。

第4図はデータパッケージ化プログラムのデータ流れ図である。

第5図はヘッダファイルの例である。

第6図は使用データファイルの例である。

第7図はデータ対象の供給者のデータプロセッサに対してローディングを行うデータ流れ図である。

第8a図および第8b図は、それぞれ、データ対象の供給者のデータプロセッサでのデータ対象のため、およびユーザに転送される準備にある対象のための制御データの例である。

第9図はデータ対象の供給者のデータプロセッサでのデータパッケージ化のデータ流れ図である。

第10図はデータパッケージ化プログラムの流れ図である。

第11図はデータ対象およびその制御データのメモリイメージである。

第12a図は連結された制御データおよびデータ対象のメモリイメージである。

。

第12b図は連結されかつ暗号化された制御データおよびデータ対象のメモリイメージある。

第13図はユーザのデータプロセッサのシステムブロック図である。

第14図は本発明によるユーザプログラムの別のモジュールを示すブロック図である。

第15図はユーザのデータプロセッサでデータ対象を使用する流れ図である。

第16図は特定の応用例においてユーザプログラムがどのように動作するかの流れ図である。

第17図は複合対象のための種々のデータパッケージ構造の例である。

発明を実現する基本モードの説明

全体概要

第1図は本発明による全体的なデータの流れを示す流れ図である。この流れ図はデータ対象供給者部分1およびユーザ部分2に分割される。

データ対象供給者部分1において、データ対象24は著者によって作られる。

データ対象はデジタルデータ、アナログデータ、あるいはアナログおよびデジタルデータの組合せもしくは混成からなることができる。アナログデータ対象とデジタルデータ対象との間の主たる相違は記憶、転送および使用のための手段にある。

著者は、また、ユーザによるデータ対象24の使用のための条件42を決定する。データ対象24および使用条件42はデータパッケージ化プログラム19に入力され、これは入力使用条件42に基づいた、データ対象および制御データの安全なデータパッケージ40を作成する。この態様で一旦パッケージ化されると、データ対象はユーザプログラム35によってのみアクセス可能となる。

データ対象は、データ対象の全体のユーザに対して同一である全体の組の制御データと共にパッケージ化されることができる。これは、データ対象が小売業者あるいは掲示板に送られそこからユーザがそれを得ることができるような場合であってもよい。また、データ対象はその使用のためのユーザからの要請の結果としてパッケージ化されてもよい。その場合に、パッケージはそのユーザに特に適応された制御データを含んでもよい。この制御データはユーザの組の制御データと呼ばれる。それは、例えば、ユーザが購入する使用の数を備えてもよい。典型的に、ユーザの組に制御データは全体の組の制御データに基づいて作られ、少なくともそのサブセットを含んでいる。ユーザの組の制御データは特定のユーザに常に適応するとは限らない。全体の組の制御データに基づいて作られた全ての組の制御データはユーザの組の制御データと呼ばれる。従って、組の制御データはある局面では全体の組のものとなり、他の局面ではユーザの組のものとなり得る。

上述したデータパッケージ化はデータパッケージ化プログラム19によって著者自身により行われることができる。別態様として、著者は自己のデータ対象をブローカに送り、そのブローカは安全なパッケージ3を作るようにデータ対象と

著者によって決定された使用条件とをデータパッケージ化プログラム19に入力するようにすることができる。また、著者は自己のデータ対象をブローカに販売するようにしてもよい。その場合に、ブローカは彼自体の使用条件をデータパッケージ化プログラムに適用することを欲する可能性がある。著者は、また、ブローカにデータ対象を安全なパッケージで供給し、ブローカはデータ対象をパッケージ解除して自己のビジネス活動に関連した一層の制御データを加えるようにしてもよい。上述の変更の全ての組合せも考えられる。

流れ図のユーザ部分2において、安全なパッケージ40はユーザによって受けられ、ユーザはこの安全なパッケージをパッケージ解除して使用のための最終形態のデータ対象80を得るためにユーザプログラム35を使用しなければならない。

本発明によるシステムの種々の部分および方法の種々のステップがここでより詳細に記載される。

データ供給者のデータプロセッサ

第2図はデータ対象の供給者のデータプロセッサのシステムブロック図である。上述したように、データ対象の供給者はデータ対象の著者、データ対象の所有者、データ対象のブローカ、あるいはデータ対象の使用の制御を留保したままデータ対象を配布することを欲する他の誰かであってもよい。データプロセッサは汎用あるいは特殊目的のプロセッサ、好ましくはネットワーク機能を備えたものである。それは、CPU10、メモリ11およびネットワークアダプタ12を具備してもよく、これらはバス13によって相互接続されている。第2図に示されているように、ディスプレイ14、キーボード15、プリンタ16、大規模記憶装置17およびROM18のような他の通常の手段もバス13に接続されてもよい。メモリ11はネットワークおよび電気通信プログラム21とオペレーティングシステム（OS）23とを記憶している。上述した要素の全ては当業者にとって周知であり、市場で入手可能である。本発明の目的のため、メモリ11は、また、データパッケージ化プログラム19と、好ましくは制御データのために意図されたデータベース20とを記憶している。現在の動作に応じて、1つあるいは

それ以上のデータ対象２４が図示されるようにメモリ１１にあるいは大規模記憶装置１７に記憶されることができる。データ供給者のデータプロセッサは安全であるものとする。

データパッケージ化プログラム

データパッケージ化プログラム１９はデータ対象の使用を制御するための制御データを作るため、ならびにデータ対象および制御データを安全なパッケージに

パッケージ化するために使用される。第３図に示されるように、それはプログラム制御モジュール３０１とユーザインターフェースモジュール３０２とパッケージ化モジュール３０３と制御データ作成モジュール３０４と暗号化モジュール３０５と１つあるいはそれ以上のフォーマットモジュール３０６と１つあるいはそれ以上のセキュリティモジュール３０７とからなる。

制御モジュール３０１は他のモジュールの実行を制御する。ユーザインターフェースモジュール３０２はデータ対象供給者とのインタラクションを取り扱う。パッケージ化モジュール３０３は制御データとデータ対象とをパッケージ化する。それは制御データ作成モジュール３０４、フォーマットモジュール３０６、セキュリティモジュール３０７および暗号化モジュール３０５を後に詳細に記載するように用いる。

作成モジュール３０６はデータ対象をそれらの本来のフォーマットで取り扱うために必要なプログラムコードを備えている。それらはデータ圧縮およびデータ変換のような機能を満たすことができる。それらは、それぞれ、ピーケーウェア社（ＰＫＷＡＲＥ　ＩＮＣ．）のウインドウズ用データ圧縮ライブラリからのルーチンおよびハンドメード・ソフトウェア社（Ｈａｎｄｍａｄｅ　Ｓｏｆｔｗｅａｒ　Ｉｎｃｏｒｐｏｒａｔｅｄ）からのイメージ鍰金術パッケージによるような任意の適切な市場で入手可能なプログラムによって実現され得る。また、これらは特注設計したプログラムによっても実現され得る。

セキュリティモジュール３０７は、データパッケージに内在する基本的なセキュリティを越えかつそれ以上の、暗号化モジュール３０５によって与えられるものよりも精巧な暗号化、許可アルゴリズム、アクセス制御および使用制御のよう

なセキュリティを実現するために必要なプログラムを備えている。

データパッケージプログラム19は多くの異なった形式のフォーマットおよびセキュリティの両モジュールを含むことができる。プログラム制御モジュール301はデータ供給者によって要求されるフォーマットおよびセキュリティモジュールを使用する。

暗号化モジュール305は、クレッセント・ソフトウェア（Crescent Software）のウインドウズ用クイックバックプロフェッショナルに見い出される「ファイルクリプト」ビジュアルベーシックサブプログラムーFILECRIPT.BASあるいは特注設計された暗号化プログラムのような任意の適切な、市場で入手可能なモジュールであってもよい。

制御データ作成モジュール304はデータ対象の使用を制御するための制御データを作成する。制御データの構造の例が次により詳細に記載される。

制御データ

制御データはヘッダファイルおよび使用データファイルに記憶されることができる。好適実施例において、ヘッダファイルは対象識別子を記憶するフィールドを備えており、この対象識別子は制御データおよび／またはその関連したデータ対象、タイトル、フォーマットコード、ならびにセキュリティコードを一意に識別する。フォーマットコードは使用データファイルでのフィールドのフォーマットあるいは位置を表してもよい。別態様として、フォーマットコードはデータパッケージ化プログラムあるいはユーザプログラムによって使用されるべき1つあるいはそれ以上のフォーマットモジュールを表すようにしてもよい。セキュリティコードは暗号化モジュール305、あるいはデータパッケージ化プログラムおよびユーザプログラムによって使用されるべき任意のセキュリティモジュールで使用される暗号化方法を表すようにしてもよい。ヘッダファイルフィールドはヘッダ要素として言及される。

使用データファイルはデータ対象の使用を制御するデータを記憶するための少なくとも1つのフィールドを具備する。データ対象の使用のための1つの条件を表す1つあるいはそれ以上の使用データフィールドは使用要素として言及される

。好適実施例において、各使用要素は、例えば連続番号といった識別子フィールド、使用要素のサイズをバイトあるいは任意の他の適切な態様で特定するサイズフィールドおよびデータフィールドによって定められる。

ヘッダ要素および使用要素は対象の使用に関連する全ての動作を制御する制御要素である。制御要素の数は制限されない。データ供給者はデータ対象の自己の所定の使用条件をを表すように任意の数の制御要素を定めることができる。唯一の制約は、データパッケージ化プログラム19およびユーザプログラム35が全ての制御要素を取り扱うために互換性があるプログラムコードを持たなければならないことである。このプログラムコードは以下に記載されるようにパッケージ化モジュールおよび使用管理モジュールに属する。

制御要素はデータ、スクリプトあるいはプログラムコードを含むことができ、これは関連データ対象の使用を制御するようにユーザプログラム35によって実行される。スクリプトおよびプログラムコードはユーザのプロセッサで関連対象およびシステムパラメータと共に処理される条件記述等を含むことができる。それは、また、特定のブローカからだけ得られることができる特定の専売ユーザプログラムを特定化するために制御要素を使用することも可能となる。

上に記載した制御データ構造は1つの例に過ぎないことが明白である。制御データ構造は異なった制御要素に関連し多くの異なった態様で定められ得る。例えば、ヘッダデータおよび使用データにおいて制御データのパーティション化は必須ではない。更にまた、上述した制御要素は一例に過ぎない。制御データフォーマットは一意のもの、例えば異なったデータ供給者に対して異なったものであって、規格に従って定められてもよい。

データパッケージ化プログラムの動作

データパッケージ化プログラムの第1の実施例の動作が第3図のブロック図および第4図の流れ図に関連して次に記載される。

最初に、データ供給者はデータ対象を作成し、それをファイルにセーブする（ステップ401）。データパッケージ化プログラムが始動されると（ステップ402）、ユーザインターフェースモジュール302は、例えば対象識別子、デー

タ対象のタイトル、データ対象のフォーマットを変換するために使用されるべきフォーマットモジュールがあればこれを特定するフォーマットコード、データ対象に一層のセキュリティを加えるために使用されるべきセキュリティコードがあればこれを特定するセキュリティコードからなるヘッダ情報をデータ対象の供給者が入力するように催す（ステップ４０３）。更にまた、ユーザインターフェースモジュール３０２は、例えばデータ対象の使用に対するデータ対象供給者の条件のような使用情報をデータ対象の供給者が入力するように催す。使用情報は、データ対象を使用することを許可されているユーザの種類、対象の種々の使用のための価格等を含んでもよい。所定のコードの形で入力されてもよいヘッダ情報

およびユーザ情報は、次いで制御モジュール３０１に与えられ、この制御モジュール３０１はパッケージ化モジュール３０３を呼出し、情報をそれに与える。

パッケージモジュール３０３は制御データ作成モジュール３０４を呼出し、これは最初にヘッダファイルを作成し、次いでデータ対象の供給者によって入力されたヘッダ情報に基づいてヘッダ情報を作成し、最後にヘッダデータを記憶する（ステップ４０４－４０５）。次いで、使用データファイルが作成され、使用データがデータ供給者によって入力された使用情報に基づいて作成され、最後に使用データが使用データファイルに記憶される（ステップ４０６－４０７）。

次いで、パッケージ化モジュール３０３はヘッドファイルにおいて特定されたフォーマットおよびセキュリティモジュール３０６、３０７があればこれをデータ対象に与える（ステップ４０８－４１３）。

次に、パッケージ化モジュール３０３は使用データファイルとデータ対象とを連結し、その結果を一時的ファイルとして記憶する（ステップ４０１）。パッケージ化モジュール３０３は暗号化モジュール３０５を呼出し、これは一時的ファイルを暗号化する（ステップ４１５）。セキュリティのレベルは使用される暗号化およびキー方法の品位に幾分か依存する。

最後に、パッケージ化モジュール３０３はヘッダファイルと暗号化された一時的ファイルとを連結し、この結果を単一のファイルとしてセーブする（ステップ４１６）。この最終的なファイルはデータパッケージとなり、これは、この際に

、ネットワークでの転送により、CD-ROMもしくはディスケットのような記憶媒体で、またはある他の手段により配布されることができるようになる。

例1

データパッケージ化プログラム19がどのようにして使用され得るかの一例が第5図および第6図に関連して次に記載される。この例において、データ対象の供給者はコンピュータグラフィックアーティストであり、このアーティストはクリップアートとして使用され得る画像を配布することを望んでいるが、ただ、本発明の方法によりパッケージ化され、しかも切り貼り処理を加えることを禁止する使用条件を有する文書あるいはファイルの形でそれを行うことを望んでいるものとする。このアーティストは画像の自由な閲覧は認めるが、ユーザが非制限的

使用に対してかなり相当の料金を支払う意志がなければ、1使用当りに基づいて支払われることを望んでいる。アーティストは自己のデータプロセッサへのダイアル呼出しラインで支払いおよび使用許可を取り扱う。

アーティストは自己の画像を作るためにアドビの（Ａｄｏｂｅ’ｓ）フォトショップといったある画像作成アプリケーションを用いる。次いで、アーティストは、グラフィカル・インターチェンジ・フォーマット（ＧＩＦ）のような配布に適切なフォーマットでファイルするために画像をセーブする。次いで、アーティストは自己のパッケージ化プログラムを始動し、対象識別子、タイトル、フォーマットコードおよびセキュリティコードを入力するが、これらはこの例で、それぞれ「１２３４５６７８９」、「画像」、「ａ」および「ｂ」である。この例において、フォーマットコード「ａ」はフォーマットコードが不用であることを表し、ＧＩＦフォーマットが適切でかつ既に圧縮されているために、このコードが選択される。更にまた、セキュリティコード「ｂ」はセキュリティモジュールが適用される必要があることを表し、暗号化モジュール３０５により行われる暗号化によって達成されるセキュリティがこのアーティストにとって適切であると考えられるためにこのコードが選択される。

次いで、アーティストは自己のダイアル呼出し電話番号、画像の単一使用およびデータ対象の非制限的使用のための価格、承認される使用形式のためのおよび

承認される使用数のためのコードを入力する。この目的のため、ユーザインターフェースモジュール３０２がデータ入力形態を表示してもよい。

データパッケージ化プログラム１９はアーティストにより入力された情報に基づいて制御データを作り、それぞれ第５図および第６図に示されるようにデータをヘッダファイルおよび使用データファイルに記憶する。このデータは全体の組の制御データを構成し、これは特別には単一のユーザには適応されないが、全ての未来のユーザに対してアーティストによって決定される使用条件を表す。

次いで、パッケージ化プログラム１９は安全なパッケージを達成するように第４図のステップ４１４－４１６に従ってデータ対象と制御データとを連結する。ヘッダファイルのデータに従って不用となるために、フォーマットモジュールもセキュリティモジュールもデータ対象には適用されない。

安全なパッケージが得られると、アーティストはそれを掲示板に送り、ユーザはそれを掲示板から検索することができるようになる。

例２

以下で、データパッケージ化プログラム１９の他の実施例が第７－１２ｂ図に関連して記載される。この例において、データ対象はビデオフィルムからなり、それはフィルム会社によって作られて、ビデオの使用のための所定の条件４２と共にブローカに送られる。ブローカはこのビデオを自己のデータプロセッサの大規模記憶装置１７にロードする。次いで、ブローカは、フィルム会社によって指示された所定の使用条件に基づいて全体的な組の制御データ５０を作るために自己のデータパッケージ化プログラム１９を使用する。更にまた、大規模記憶装置１７内のビデオへのアドレスは制御データベース２０のアドレステーブルにあるいはメモリ１１の外の他の場所に記憶される。それは、また、全体的な組の制御データ５０に記憶されることもできる。最後に、この全体的な組の制御データは制御データベース２０に記憶される。また、それはメモリ１１の外の他の場所にも記憶されることができる。第４図のステップ４０１－４０７に対応するこれらの動作の後に、データパッケージ化プログラムが始動される。

第８ａ図はこの例によるビデオのための全体的な組の制御データを示す。ここ

で、制御データは識別子、フォーマットコード、セキュリティコード、使用要素の数、データ対象のサイズ、使用要素のサイズ、2つの使用要素（それぞれが識別子フィールド、サイズフィールドおよびデータフィールドからなる）を含んでいる。識別子は特定のブローカに対して登録された一意の連続番号であってもよい。この例において、識別子は「１２３４５６７８９」であり、フォーマットコードは「００１０」で、これは、この例でＡＶＩビデオのフォーマットを表し、セキュリティコードは「００１０」である。更にまた、第１の使用要素はビデオのための受け入れられるユーザを定め、第２のユーザ要素のデータはユーザが購入するビデオの視聴回数を定める。第１の使用要素のデータは１であり、これは、この例の目的のため、教育関係のユーザのみがフィルム会社に受け入れられるということを表す。第２のユーザ要素データのデータフィールドは、この段階でビデオの視聴が購入されていなかったために空白である。

対象の転送の管理

ブローカはデータ対象をユーザに転送し、使用代金あるいはロイヤリティの支払いの返答として制御された使用を可能とすることを欲する。ブローカ対ユーザのビジネス関係を管理し、ブローカとユーザ間の取引を行わせることは共に自動的になされることができ、制御データ構造はこれら動作に対して無制限のサポートを与えることができる。支払いはクレジットカード情報を送信することによって取り扱われることができ、あるいはユーザはパスワードで起動して、引落しおよびブローカとの借方勘定を持つことができる。好ましくは、支払いはデータ対象がユーザに転送される前に確認されるべきである。

データパッケージ化

ユーザがデータ対象を使用することを欲すると、ユーザはブローカに連絡して、そのデータ対象の使用の許可を要求する。この許可要求がブローカのデータプロセッサで受けられると、データプログラムは許可を必要とする使用とデータ対象の制御データの使用制御要素とを比較し、それがそこに指示されている所定の使用条件に従っているかどうかを調べる。この比較はユーザ形式、使用形式、使用回数、価格等を比較することを含んでもよい。要求された使用が所定の条件に

従っていれば、許可が与えられ、そうでなければそれは拒絶される。

第9図はブローカのデータプロセッサでのデータパッケージ化のデータ流れ図であり、これは、ビデオの使用許可に対するユーザからの承認された要求に応じて、例えば2回の視聴の購入に対する許可された要求に応じて生じる。

許可された要求に応じて、ブローカは再度データパッケージ化プログラム19を適用する。全体の組の制御データ50およびデータ対象24はそれぞれ制御データベース20および大規模記憶装置17からプログラムに入力される。プログラム全体の組の制御データ50に基づいてユーザの組の制御データ60を作り、ユーザの組60とデータ対象24を連結して安全なデータパッケージ40を作るが、これは次いで任意の好ましい手段によりユーザに転送されることができる。好ましくは、ユーザの組の制御データのコピーがブローカの制御データベースに記憶される。これは以後の使用との、例えばダイアル呼出しがいつ使用に対して要求されるかの比較を行うためのレコードをブローカに与える。

第10図はユーザの組の制御データを作るためおよびユーザの組の制御データおよびビデオを安全なパッケージにパッケージ化するために使用される例示的なプロシージャの流れ図である。ここで、プロシージャは第8a図に示される全体的な組の制御データに関連して記載される。

ユーザの組の制御データ、すなわちこの例の特定のユーザに適応される制御データの組は第11図のステップ1001－1003によって作られる。最初に、制御データベースに記憶されている全体の組の制御データ50は新たな制御データを作るためにコピーされる（1001）。第2に、ユーザの組の制御データを一意に識別する新たな識別子（ここでは、「1234567890」が新たな制御データ60の識別子フィールドに記憶される（ステップ1002）。第3に、第2の使用要素のデータフィールドは購入された使用、すなわちこの例では、ビデオの2回の視聴が購入されたため2で更新される（ステップ1003）。

第8aの全体の組の制御データに対応するこのようにして作られたユーザの組の制御データは第8b図に示されている。

ユーザの組の制御データは制御データベース20に記憶される（1004）。

次いで、大規模記憶装置17に記憶されているビデオがコピーされる（ステップ1005）。ビデオのこのコピーはユーザの組の制御データと連結される（ステップ1006）。セキュリティコード0010は全体のデータパッケージ40が暗号化されるべきこと、およびユーザプログラム35が付与されることができるキーを含まなければならないことを指定する。従って、全体のデータパッケージは暗号化される（ステップ1007）。最後に、暗号化されたデータパッケージはユーザへ更に転送するため、記憶媒体に記憶されるか、あるいはネットワークプログラムに与えられる（1008）。

第11図はビデオ24およびユーザ制御データ60のメモリイメージである。ユーザ制御データおよびビデオ24のコピーは第12a図に示されるように連結される。暗号化されたデータパッケージ40は第12b図に示されている。

第10図のプロシージャは第3図のデータパッケージ化プログラムによって実行されることができる。第10図のプロシージャに対する別態様として、ユーザの組の制御データはステップ1001－1003の場合に作られ、ヘッダファイルおよび使用データファイルにセーブされることができ、その後に第4図のデータパッケージ化プログラムのステップ408－416が安全なパッケージを作るために行われることができる。

ユーザ適応の組の制御データを作るための上述のプロセスは、また、データ対象を再配布することを欲しているユーザによってあるいは他のブローカにデータ対象を配布することを望んでいるブローカによって使用されてもよい。明かに、データ対象の再配布は、それがデータ対象の制御データにおいて承認された使用であることを必要とする。そうであれば、ユーザあるいはブローカは新たな制御要素を加えることによって、可能ならば古い制御要素のデータフィールドを変えて著者と現在のユーザ／ブローカとの間のならびに現在のユーザ／ブローカと将来のユーザ／ブローカとの間の関係を反映することによってユーザの組の制御データを作る。この態様で、監査証跡が作られる。

ユーザのデータプロセッサ

第13図に示されるユーザのデータプロセッサは、好ましくはネットワーク機

能を備えた汎用あるいは特殊目的のプロセッサである。それはＣＰＵ２５、メモリ２６およびネットワークアダプタ２７を備え、これらはバス２８によって相互接続されている。第１３図に示されているように、ディスプレイ２９、キーボード３０、プリンタ３１、サウンドシステム３２、ＲＯＭ３３および大規模記憶装置３４のような他の通常の手段もバス２８に接続されてもよい。メモリ２６はネットワークおよび電気通信プログラム３７とオペレーティングシステム（ＯＳ）３９を記憶している。全ての上述した要素は当業者にとって周知で、市場で入手可能である。本発明の目的のため、メモリ２６は、また、ユーザプログラム３５および好ましくは制御データのために意図されたデータベース３６をも記憶している。現在の動作に応じて、データパッケージ４０は図示されるようにメモリ２６にあるいは大規模記憶装置３４に記憶されることができる。

ユーザプログラム

ユーザプログラム３５は制御データに従ってデータ対象の使用を制御し、この制御データはデータ対象と共にデータパッケージに含まれている。

第１４図に示されるように、ユーザプログラム３５はプログラム制御モジュール１４０１とユーザインターフェースモジュール１４０２と使用管理モジュール１４０３と制御データパーサモジュール１４０４と暗号解読モジュール１４０５と１つあるいはそれ以上のフォーマットモジュール１４０６と１つあるいはそれ以上のセキュリティモジュール１４０７とファイル転送プログラム１４０９とからなる。

制御モジュール１４０１は他のモジュールの実行を制御する。ユーザインターフェースモジュール１４０２はユーザとのインクラクションを取り扱う。使用管理モジュール１４０３は安全なパッケージ４０をパッケージ解除する。それは制御データパーサモジュール１４０４、暗号解読モジュール１４０５、フォーマットモジュール１４０６、およびセキュリティモジュール１４０７を用いる。

フォーマットモジュール１４０６は、圧縮解除およびデータフォーマットプロシージャのような、データ対象をそれらの本来のフォーマットで取り扱うために必要なプログラムコードを備えている。セキュリティモジュール１４０７は、ア

クセス制御、使用制御および基本的暗号解読モジュール１４０５によって与えられるものよりもより精巧な暗号解読のような、最も低いレベル以上のセキュリティを実現するために必要なプログラムコードを備えている。

ユーザプログラム３５は多くの異なった形式のフォーマットおよびセキュリティの両モジュールを含むことができる。しかしながら、それらは対応するデータパッケージプログラムにおいて使用されたフォーマットおよびセキュリティモジュールと相補的でなければならない。使用管理モジュール１４０１は、データ対象を使用するために必要でありかつその制御データにおいて特定されるフォーマットおよびセキュリティモジュールを適用する。適切なフォーマットおよびセキュリティモジュールが特定のデータ対象に対して利用できなければ、使用管理モジュール１４０１は一切の使用を許可しない。

暗号解読モジュール１４０５は、上述したファイルクリプト・ビジュアルベーシックのサブプログラムあるいはある他の市場で入手可能な暗号解読プログラムにすることができる。それは、また、特注設計された暗号解読プログラムであってもよい。ユーザプログラムで使用される暗号解読モジュールがデータパッケージ化プログラムの暗号化モジュールと相補的であることが単に制限であるに過ぎない。

制御データパーサモジュール１４０４は第３図の制御データ作成モジュール３０４の逆プロセスを行う。

ユーザプログラム３５はパスワードあるいは任意の他の好ましい方法によるプログラムの使用を制御するコードを有することができる。パスワードはデータ対象のパッケージ化の間にパスワード制御要素に加えられてもよい。パスワードは書留郵便あるいは任意の他の適切な態様でユーザに送られる。制御データ構造にパスワード制御要素が存在することに応じて、ユーザプログラムはユーザにパスワードを入力することを催す。入力されたパスワードは制御データ内のパスワードと比較され、それらが一致すれば、ユーザプログラムはそのまま続き、そうでなければそれは無能化される。

ユーザプログラム３５は、また、ユーザ対象４１の制御データに従ってプログ

ラムの振舞いを変える（例えば、子供に対するフィルタを設ける）プロシージャを有することができる。ユーザプログラム３５はユーザがアクセス可能な記憶装置に対象を本来のフォーマットで決して記憶せず、かつデータ対象の表示の間にプリントスクリーンキーがトラップされるということを言及することが重要である。

ファイル転送プログラム１４０９はネットワークを介して他のデータプロセッサへのおよびそれからのファイルを転送および受信することができる。

データ対象は使用の後に安全なパッケージに再パッケージ化されるために、ユーザプログラムは、また、データ対象を再パッケージ化するためのプログラムコードを含まなければならない。このプログラムコードは対応するデータパッケージ化プログラム１９において使用されたものと同じにすることができよう。それは、また、ユーザプログラムから呼ばれる別のプログラムにすることもできる。

ユーザプログラムの動作

ユーザプログラム３５の実施例の動作が第１４図のブロック図および第１５図の流れ図に関連して次に記載される。

最初に、ユーザはデータパッケージ４０をネットワークを介するファイル転送によりあるいはＣＤ－ＲＯＭもしくはディスケットのような記録媒体で、または

任意の他の適切な手段によりデータパッケージ４０を受け取る（ステップ１５０１）。次いで、ユーザは自己のデータプロセッサでこのデータパッケージをファイルとして記憶する（ステップ１５０２）。

ユーザがデータ対象を使用したい時には、ユーザプログラム３５を始動する（ステップ１５０３）。要求がユーザインターフェースモジュール１４０２によって受けられ、これは制御モジュール１４０１にユーザ要求を知らせる。制御モジュール１４０１は使用管理モジュール１４０３を呼出し、使用要求を引き渡す。

使用管理モジュール１４０３はデータパッケージからフォーマットコードを読み、制御データフォーマットを決定する。次いで、それは暗号解読モジュール１４０５を呼び出してデータパッケージから制御データを暗号解読および抽出する。使用管理モジュール１４０３は制御データのみを暗号解読するように暗号解読

モジュール１４０５を増進的に適用する。最後に、それは制御データをメモリに記憶する（ステップ１５０５）。

使用管理モジュール１４０３は、次いで、制御データパーサモジュール（ｄａｔａ　ｐａｒｓｅｒ　ｍｏｄｕｌｅ）を呼出し、使用要素からデータフィールドを抽出する。

次いで、使用管理モジュール１４０３は使用のためのユーザ要求と対応する制御データとを比較する（ステップ１５０６－１５０７）。要求された使用が制御データにおいて許可されなければ、要求された使用は無能化される（ステップ１５０８）。しかしながら、要求された使用が制御データにおいて承認されたならば、使用管理モジュール１４０３はヘッダデータあるいは使用データで指定されたフォーマットおよびセキュリティモジュール１４０６、１４０７があればこれをデータパッケージに適用する（ステップ１５０９－１５１４）。

次いで、使用管理モジュール１４０３は暗号解読モジュール１４０５を呼び出し、この暗号解読モジュールは対象データを暗号解読し（ステップ１５１５）、その後に要求された使用が可能とされる（ステップ１５１６）。使用の可能化に関連して、制御データは更新されることが必要であってもよい（ステップ１５１７）。制御データは、例えば制限された数の使用を指示するデータフィールドを具備してもよい。そうであった場合に、このデータフィールドは使用の可能化に応じて１だけ減少される。ユーザがデータ対象の使用を完了すると、使用プログラム３５はデータ対象を再パッケージ化することによって安全な形態にデータパッケージを元に戻す（ステップ１５１８）。より詳細には、データ対象および使用要素は連結されて、再暗号化される。次いで、ヘッダ要素が加えられ、このようにして作られたパッケージはユーザのデータプロセッサに記憶される。

例１（続き）

ユーザプログラムがどのようにして動作するかの特定の例が第６図および第１５図に関連して次に記載される。この例は上の例１の続きであり、アーティストが画像を作成して、それを掲示板に送る場合である。

ユーザが電子掲示板（ＢＢＳ）でその画像を見い出してそれを使うことに興味

を持ったものと想定する。次いで、ユーザはその画像を含んだデータパッケージ４０を自己のデータプロセッサにロードし、大規模記憶装置にそれをファイルとして記憶する。次いで、ユーザはユーザプログラム３５を実行し、その画像を予備的に見ることを要求する。次いで、ユーザプログラムは第１５図のステップ１５０５－１５０７を実行する。画像を予備的に見るための要求は使用要素のデータフィールド（承認された使用形式のためのコード）と比較される。この例において、コード「9」は予備的に見ることが行われることを表す。このようにして、要求された予備的に見ることはＯＫである。次いで、ユーザプログラム３５は第１５図のステップ１５９８－１５１５を行う。ヘッダデータのフォーマットコード「a」およびセキュリティコード「b」は変換も圧縮解除もセキュリティ処理も必要でないことを指示するために、ユーザプログラムは対象データを単に暗号解読するに過ぎない。次いで、使用管理モジュール１４０３はユーザのデータプロセッサに試読画像を表示し、ユーザインターフェース１４０２に制御を戻す。

ユーザが画像を予備的に見ることを終了したら、ユーザインターフェースモジュール１４０２は制御データの価格使用データ（第６図において「単一使用の価格」および「非制限的使用の価格」）に従って画像の使用コストを表示し、ユーザによる購入要求の入力を待機する。ユーザは画像の非制限的使用を買うことを決定し、ユーザインターフェースモジュール１４０２は識別子、支払い請求およびその要求に対するアドレスのような購入情報を入力すると、その要求は制御モジュール１４０１に渡される。制御モジュールはファイル転送プログラム１４０９を呼び出し、これは使用データ（第６図の「アーティストの電話番号のための制御要素」）に指示されているようにアーティストのダイアル呼出し番号をダイアルし、要求および購入情報をアーティストのデータプロセッサのブローカプログラムに転送する。購入が承諾されると、ブローカプログラムは「承認された使用形式」制御要素のための更新を含んだファイルに戻る。この更新は承認された使用形式に対して「１０」であり、これは、この例において、そのユーザによる非制限的使用が許されたことを指示する。ファイル転送プログラム１４０９はこ

の更新を使用管理モジュール１４０３に渡し、これは制御データを「承認された使用形式」コードで更新する。ユーザインターフェースモジュール１４０２は、次いで、ユーザへの確認メッセージを表示させる。

引続いて、ユーザインターフェースモジュールは本発明に従ってパッケージ化されたファイルに画像をコピーする要求をユーザの機械で入力する。次いで、使用管理モジュールはユーザ要求制御データを比較する。使用管理モジュールは、ここでは「１０」である「承認された使用形式」に対してファイルされたデータを試験する。使用管理モジュールは画像をファイルにコピーする。

ユーザが画像を使い終えると、使用管理モジュール１４０３は画像を更新された制御データを除き前のように再パッケージ化する。この再パッケージ化プロセスは、ヘッダおよび使用データが既に存在していることを除き、実際第４図に示されたものと同様であり、そのためプロセスは制御データが作られるようなステップ４０６の後に開始する。

改良されたセキュリティ

データ対象の供給者がデータ対象を含んだデータパッケージのセキュリティを向上したい場合、ＲＳＡのような精巧な暗号化アルゴリズムを含んだセキュリティモジュール３０７が使用され得る。その場合に、パッケージ化モジュール３０３は第４図の流れ図のステップ４１２でセキュリティモジュール３０７を呼び出す。セキュリティモジュールは画像を暗号化して、セキュリティアルゴリズムコードを制御データ作成モジュール３０２に引き渡し、これはセキュリティモジュールコードのための制御要素を加え、これはユーザプログラム３５によって検出

される。次いで、ステップ４１４でのデータパッケージ化が続く。データパッケージがユーザに送られると、パブリックキーがユーザに書留郵便で郵送される。ユーザプログラムがこのデータ対象の使用要求に応じて実行されると、使用管理モジュールは制御データのセキュリティモジュールコードを検出し、セキュリティモジュールを呼び出す。このモジュールはユーザインターフェースモジュール１４０２に制御を渡し、これはパブリックキーを入力するようにユーザに要求する。キーが正しければ、ユーザセキュリティモジュールはそのキーを用いて相補

的暗号解読を与え、使用管理モジュールに使用承認メッセージを引き渡し、この使用管理モジュールにより使用が可能となる。

改善されたセキュリティの他の例として、セキュリティモジュールは許可プロセスを構成することができ、これに従ってデータ対象の各使用はデータ対象供給者のデータプロセッサへのダイアル呼出しを必要とする。対応するセキュリティモジュールコードがユーザプログラム35によって検出されると、関連するセキュリティモジュールが呼び出される。このモジュールは許可要求を制御モジュール1401に渡し、これはファイル転送プログラム1409を呼び出し、このプログラムは使用要素で指示されたデータ対象供給者にダイアル呼出しを行い、使用の許可要求を転送する。承認された許可を受けると、データ供給者のデータプロセッサは使用が許可されたメッセージをユーザセキュリティモジュールに戻し、これはこの許可を使用制御モジュールに送り、これは1回の使用を可能とする。ユーザがデータ対象のそれ以上の使用を要求すれば、許可プロセスは繰り返される。この結果、このプロシージャは永久的なデータ対象のセキュリティを与える。

例2（続き）

ユーザプログラム35がどのようにして動作するかについての他の特定の例が第16図に関連して次に記載される。この例は上の例2の続きであり、それはユーザがブローカからビデオフィルムの2つの視聴物を購入した場合である。

ユーザはブローカから購入されかつ送られたビデオを見ようとしている。ユーザはユーザプログラム35を適用し（ステップ1601）、かつビデオを見ることを要求する（ステップ1602）。ユーザプログラム35は最初にユーザの組の制御データ60を検査する（ステップ1603）。この例において、ユーザプログラム35は対象のためのフォーマットおよびセキュリティモジュールのみを含むだけであり、フォーマットコードは0010で、セキュリティコードは0010である。この結果、これら形式のデータ対象だけが使用され得る。プログラムが他のコードを受ければ、使用行為は不可能となる（ステップ1604－1605）。

次に、ユーザプログラム35は、1である（教育関係ユーザだけ）第1の制御要素データをユーザプログラムの要求に応じてユーザによって入力されるユーザ情報に対して比較する。ユーザによって入力されるユーザ形式は第1の使用要素において指示されているものと同じであるために、プロセスは続く（ステップ1606－1507）。次いで、ユーザプログラムは、購入する視聴の回数が2であることを特定する第2の制御要素データをチェックする。この結果、使用が可能となる（ステップ1609）。ユーザプログラムは万能キーで暗号解除モジュールを適用し、フォーマットビデオはディスプレイユニット29に表示される。次いで、第2の制御要素データは1だけ減少される（ステップ1610）。最後に、ビデオは再パッケージ化される（ステップ1611）

可変で伸長可能な対象の制御の実現

対象の制御はデータパッケージ化プログラム19と使用プログラム35との制御データを用いるインタラクションにより達成される。制御影響変動値と影響変動値が与えられる状況とを制御要素が定めるようにして制御データフォーマットを作ることによって対象制御の影響変動値が与えられ得る。次いで、プログラムプロシージャが制御要素を処理するようにプログラムモジュールに加えられなければならない。例えば、学生は特定の論文を無料でプリントできるが、ビジネスユーザにはそれに対して支払いが必要であることをブローカが望むものとする。ブローカは、学生およびビジネスのユーザ形式とそれぞれに対する関連したコストを表す制御要素を定める。次いで、ブローカはユーザ形式を検査してそれに応じてコストを計算するプログラムロジックを加える。対象制御は、対象制御に対する基準を定めるパラメータと同じ程多くの要素を制御データフォーマットが有する方向に拡張性がある。

変動性で拡張性の対象セキュリティの実現

対象セキュリティは、また、制御データを用いてデータパッケージ化プログラム19とユーザプログラム35とのインタラクションにより達成される。セキュリティプロセスおよび暗号化／暗号解除アルゴリズムがプログラムモジュールとして加えられることができる。セキュリティ影響変動値と影響変動値が与えられ

る状況とを制御要素が定めるようにして制御データフォーマットを作ることによって対象セキュリティの影響変動値が特定の対象に与えられ得る。プログラムプロシージャが制御要素を処理するためにプログラムモジュールに加えられなければならない。例えば、ブローカが現在のニュース記事の自己による収集に対しては最少のセキュリティを適用させるが、自己の辞書および教科書には厳格なセキュリティを与えたいものとする。このブローカはセキュリティ形式のための制御要素を定める。次いで、ブローカはこれに対応してセキュリティアルゴリズムを適用するアルゴリズムロジックを加える。対象セキュリティは多レベルのセキュリティを与えることができる方向に拡張性がある。勿論、セキュリティのレベルはセキュリティモジュールにおいて実行される暗号化／キー方法に依存する。1つのレベルのセキュリティはデータ対象をユーザのデータプロセッサにロードする時にオンライン確認を必要とするようにしてもよい。これはセキュリティモジュールのプログラムコードにおいて実現されることができる。これによりブローカは対象がまだロードされていないことをチェックすることができ、かつ全ての他のパラメータを二重チェックすることができるようになる。

使用プログラムとユーザの制御データベースとの間でタイムスタンプを用いるバージョン管理を持つことも重要である。そうでなければ、データベースは二重化され、ユーザプログラムに再適用されてしまう。ユーザプログラムは、制御データベースがアクセスされる各度に、制御データベースと隠しシステムファイルにタイムスタンプを与えることができる。タイムスタンプが同一でなければ、制御データベースが調節されたことになり、全ての使用は無能化される。タイムスタンプを扱うプログラムコードはセキュリティモジュールに属することができる。

複合対象の取扱

複合対象は、制御要素が構成成分間の関係を定めるようにして制御データフォーマットを規定し、かつ親／子要素と関連した対象ＩＤ要素を規定することによって取り扱われ得る。例えば、ブローカは教育的なパッケージにビデオおよび教科書を含めることを望むものと想定する。ブローカは、制御要素がビデオおよび

教科書を言及するような親対象を作る。ブローカは、また、親対象として言及するビデオ対象および教科書対象のための制御データに制御要素を含めるようにする。最後に、ブローカは制御要素を処理するためにプログラムプロシージャプログラムモジュールに加える。

換言すれば、データ対象が少なくとも2つの構成要素データ対象を含む複合データ対象である時には、それぞれの全体の組の制御データは構成要素データ対象のそれぞれに対しておよび複合データ対象に対して作られる。

複合対象のための種々のデータパッケージ構造の例が第17図に与えられる。

複合対象の他の側は、ユーザがある特定の使用に対してデータ対象を組み合せようとする時である。この組合せは各構成要素データ対象においてなされなければならない使用行為である。制御データが構成要素データ対象と結合されるようになった新たなデータ対象が作られる。各構成要素データ対象は後の使用を制御し続けるその元の制御データを保留する。

ユーザが複合データ対象の構成要素データ対象の使用許可を要求すると、ユーザの組の制御データがその構成要素データ対象に対してだけに作られ、その構成要素データ対象のコピーとだけに連結される。

スケーリング可能な実施

融通性がある制御構造およびモジュールプログラム構造は、使用管理およびローヤリティの支払いに対する所有者の要求の実現に関して殆ど限りがない拡張性を可能とする。制御データ構造は、複雑なユーザ形式、使用形式、多支払い請求計画、芸術あるいは所有権信用取引要求およびその他のための制御要素を含むことができる。制御データ構造および制御データの任意の変更のものと作用するセキュリティモジュールを含むことができる。セキュリティモジュールはローディングあるいは使用行為を承認しかつ承認確認メカニズムを実現するためにブローカのデータプロセッサを必要とさせることができる。

ブローカとして働くユーザ

ブローカのデータパッケージ化プログラムの制限的なあるいは完全な実現はユーザの機械で、再配布あるいは再販売を可能とするように達成され得る。しかしな

がら、再配布あるいは再販売を可能とする制御データを備えたデータ対象だけをその態様で行わせることができる。

再仲介

データ対象の著者は、自己の最初のブローカが自己のデータ対象を他のブローカに配布し、その他のブローカが同様その画像を配布させるように欲してもよい。この際に、著者は、最初のブローカに関連した制御データを有するデータ対象を配布する前に、再仲介を可能とする制御要素をその制御データに含ませる。この再仲介の要請時に、最初のブローカは全体の組の制御データをコピーし、以後のブローカのデータプロセッサで全体の組の制御データとして働くユーザの組の制御データを作るようにそのコピーを更新する。最初のブローカはユーザの組の制御データを有するデータ対象をパッケージ化し、そのパッケージを以後のブローカに転送する。次いで、以後のブローカはそれが元のブローカであったとしたらそれを続ける。

自動化された取引交渉

これは、制御データに含まれた所定の使用条件が自動化された取引交渉を達成するためにどのようにして使用され得るかの例である。

ある会社がコンピュータ自動化株取引を行うことを望んでいるものとする。売買注文がデータパッケージの形で実現されることができ、ユーザプログラムはこのデータパッケージを処理し、取引を実行することができる。データパッケージはデジタルキャシュを保持し、制御データで定められた条件に基づいて支払いを管理する。

この例において、買い注文は、買い手のデータプロセッサで、本発明に従ってデータパッケージ化プログラムを用いて作られる。売り注文は売り手のデータプロセッサでデータパッケージ化プログラムを用いて作られる。両注文は株のトレーダのデータプロセッサでのユーザプログラムによって使用される。これら使用は株を売る売り注文データパッケージおよび株を買うための買い注文データパッケージの形態を取る。株を売買するための基準あるいは条件をパッケージの制御データにおいて指示することができる。データ対象はデジタルマネーからなる。

この意味で、デジタルマネーはデジタル取引のために発行されかつ維持される実際の金銭ありは架空の金銭を参照する単なるデータであることを覚えておくことが重要である。

この例において、買い手はデジタルマネーデータファイルを用いて始める。買い手は、例えば株の種類、価格、購入数量といった制御データを作るためにデータパッケージ化プログラムを使用し、次いでデジタルマネーデータファイルおよび制御データを上述したように安全なパッケージにパッケージ化する。

売り手は空きのデータファイルを用いて始める。この空きのデータファイルは、それが空であることを除き、デジタルマネーデータファイルと類似している。売り手は、例えば株の種類、数量といった制御データを作り、空きのファイルおよびこの制御データを安全なパッケージにパッケージ化する。

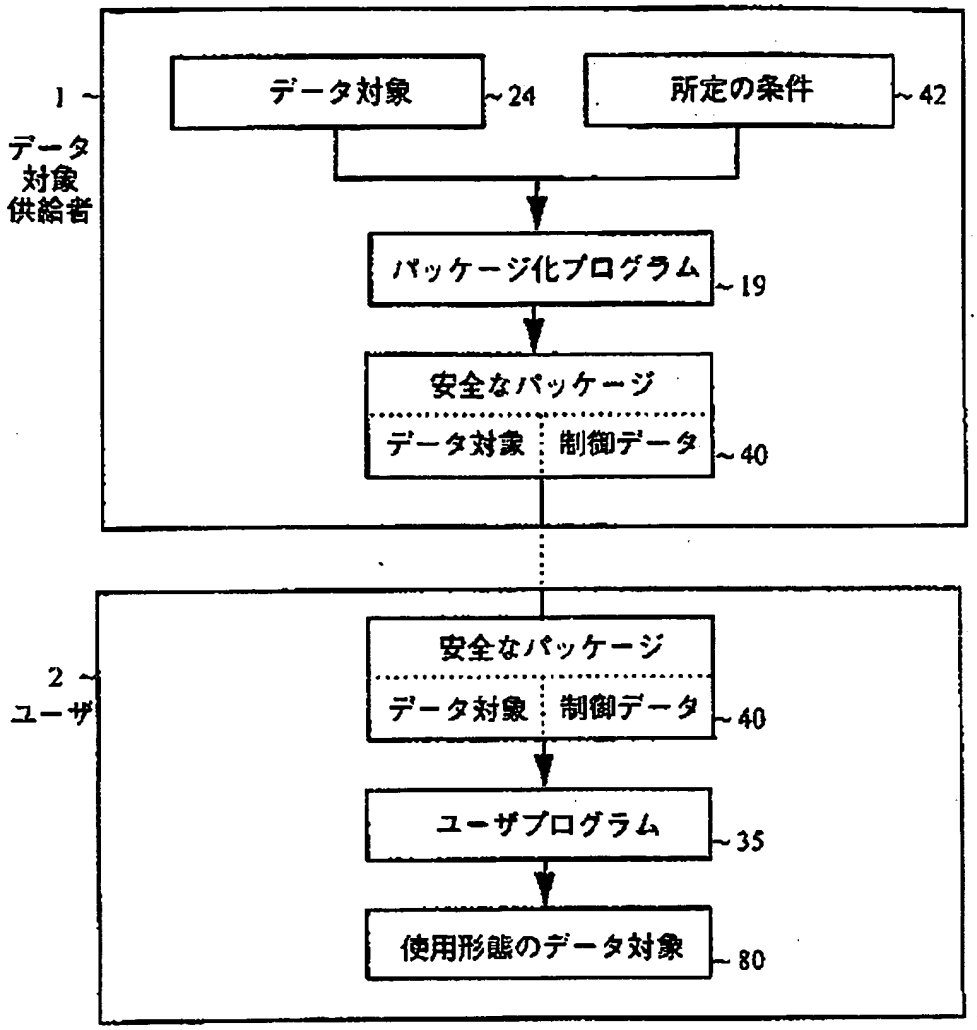
売り注文パッケージおよび買い注文パッケージの両方は株取引会社のデータプロセッサ転送され、そこでそれらが受信され、メモリに記憶される。株取引会社のユーザプログラムは売りおよび買い注文パッケージの制御データを上述したと同じ態様で検査し、一致を捜す。一致した買いおよび売り注文を識別すると、ユーザプログラムは取引を実行し、それによってデジタルマネーは買い注文データパッケージから抽出されて売り注文データパッケージに転送される。次いで、データパッケージの制御データは監査証跡を与えるように更新される。両パッケージはそれらが前にパッケージ化されたと同じ態様で再パッケージ化され、それらの著者に戻されるように転送される。

上述の技術は任意の対象を売買するためおよび自動化された交渉を行うために使用され得る。支払いはデジタルマネーによる場合以外の任意の態様で行われてもよい。

一般的な場合において、ユーザのデータプロセッサはユーザの組の制御データの使用制御要素を暗号解除し、一致を見い出すように使用制御要素を検査する。一致が見いだされることに応じて、ユーザのデータプロセッサはユーザの組の制御データで特定される行為を実行する。

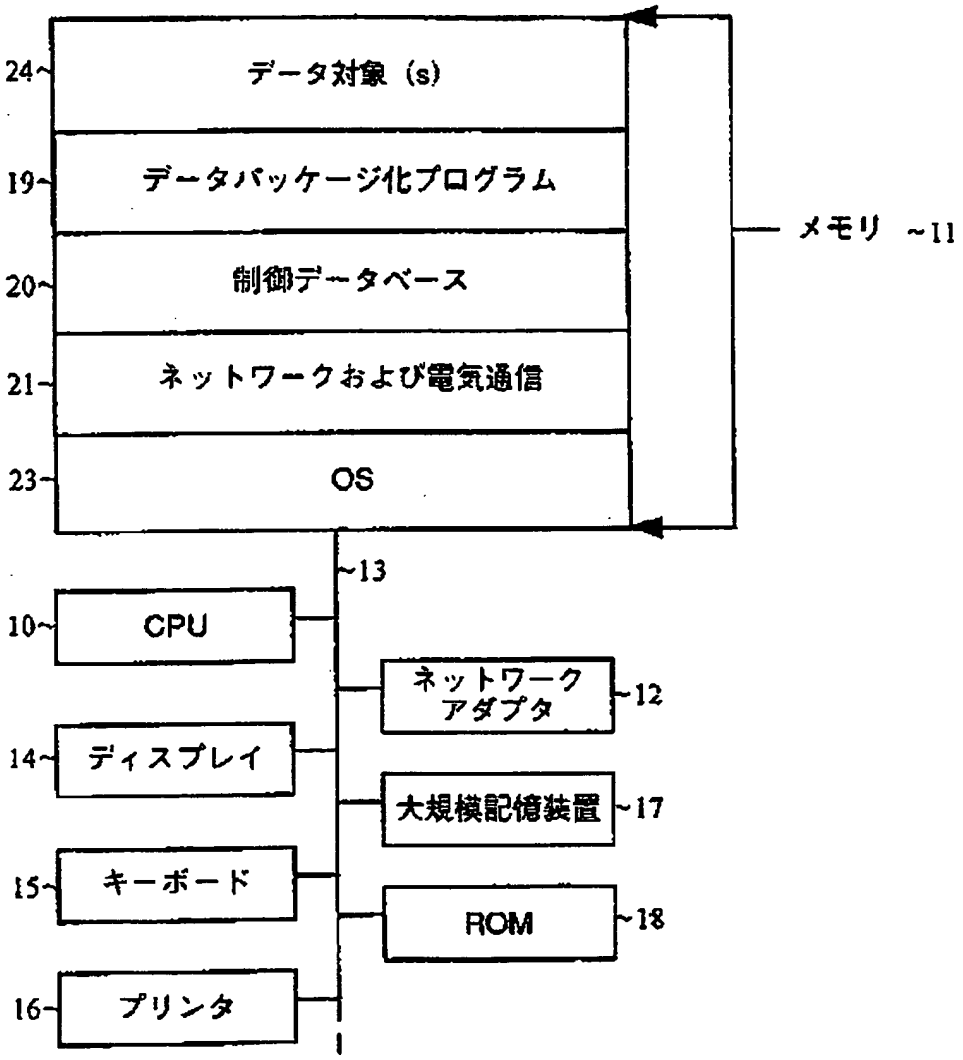
【図1】

Fig 1


1
データ対象供給者
データ対象
24
所定の条件
42
パッケージ化プログラム
19
安全なパッケージ
データ対象
制御データ
40
2
ユーザ
安全なパッケージ
データ対象
制御データ
40
ユーザプログラム
35
使用形態のデータ対象
80

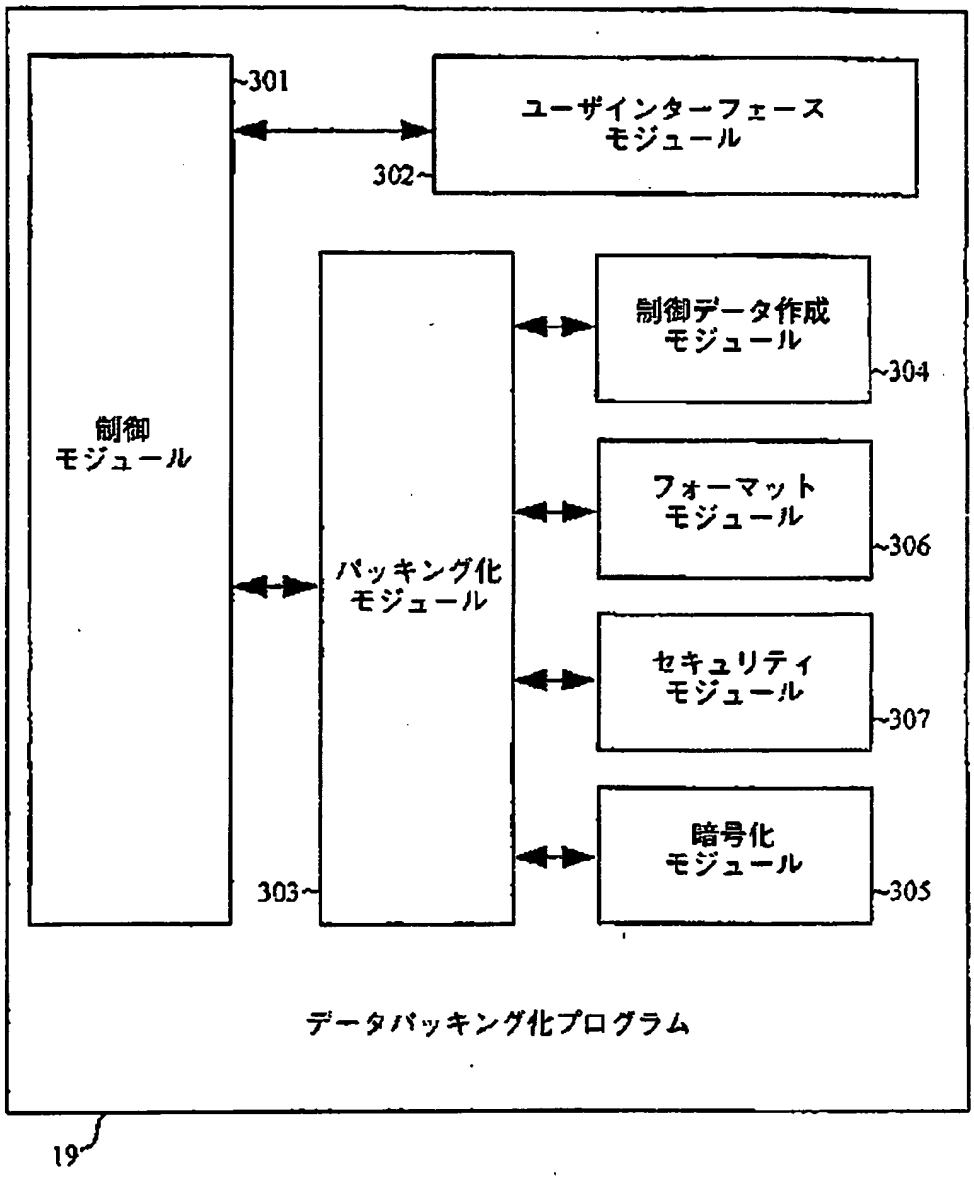
【図2】

Fig 2


24
データ対象（s）
19
データパッケージ化プログラム
20
制御データベース
21
ネットワークおよび電気通信
23
OS
メモリ ~11
~13
10
CPU
ネットワーク
アダプタ
~12
14
ディスプレイ
大規模記憶装置
~17
15
キーボード
ROM
~18
16
プリンタ

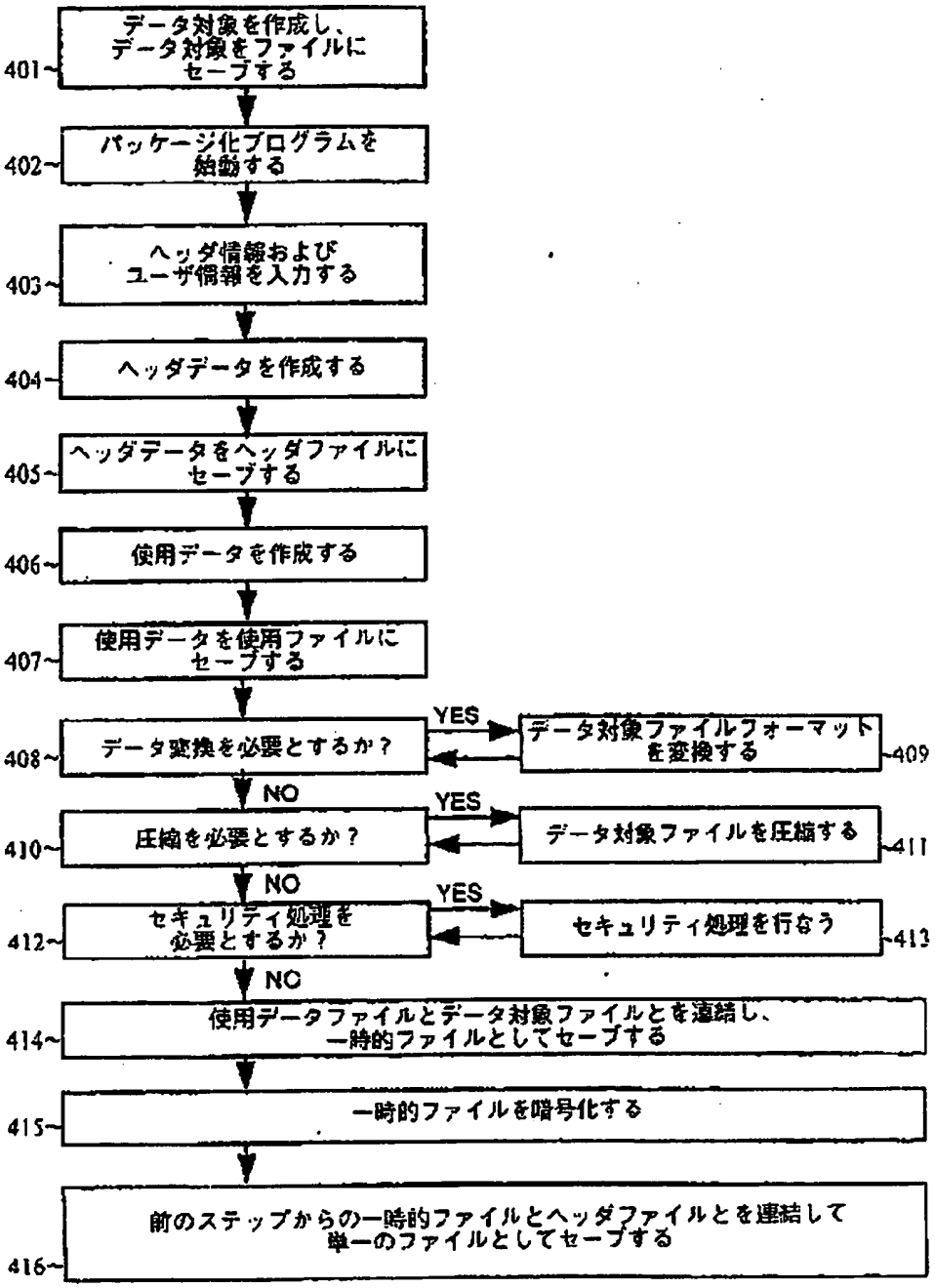
【図3】

Fig 3


301
ユーザインターフェース
モジュール
302
制御
モジュール
パッキング化
モジュール
303
制御データ作成
モジュール
304
フォーマット
モジュール
306
セキュリティ
モジュール
307
暗号化
モジュール
305
データパッキング化プログラム
19

【図4】

Fig 4


401
データ対象を作成し、
データ対象をファイルに
セーブする
402
パッケージ化プログラムを
始動する
403
ヘッダ情報および
ユーザ情報を入力する
404
ヘッダデータを作成する
405
ヘッダデータをヘッダファイルに
セーブする
406
使用データを作成する
407
使用データを使用ファイルに
セーブする
408
データ変換を必要とするか？
YES
データ対象ファイルフォーマット
を変換する
409
NO
410
圧縮を必要とするか？
YES
データ対象ファイルを圧縮する
411
NO
412
セキュリティ処理を
必要とするか？
YES
セキュリティ処理を行なう
413
NO
414
使用データファイルとデータ対象ファイルとを連結し、
一時的ファイルとしてセーブする
415
一時的ファイルを暗号化する
416
前のステップからの一時的ファイルとヘッダファイルとを連結して
単一のファイルとしてセーブする

【図5】

Fig 5

ファイル識別子	123456789
タイトル	画像
フォーマットコード	a
セキュリティコード	b

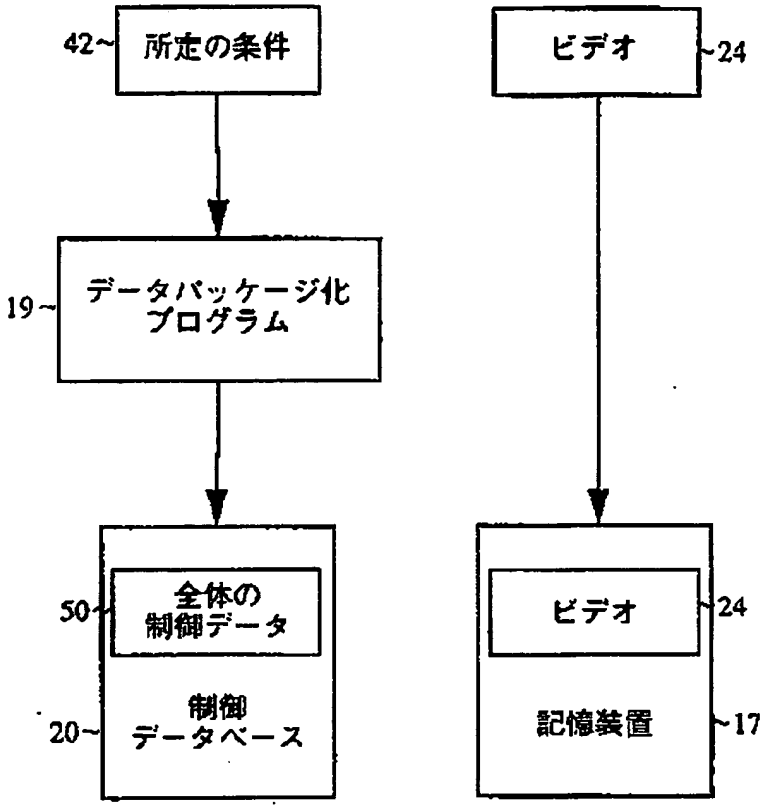
【図6】

Fig 6

著者の電話番号のための使用要素	識別子	1
	サイズ	13
	データ	716 381 5356
単一使用の価格	識別子	2
	サイズ	4
	データ	.50
非制限的使用の価格	識別子	3
	サイズ	4
	データ	50.00
承認された使用形式のためのコード	識別子	4
	サイズ	2
	データ	9
承認された使用回数のためのコード	識別子	5
	サイズ	2
	データ	1

【図7】

Fig 7


42~
所定の条件
ビデオ
~24
19~
データパッケージ化
プログラム
50~
全体の
制御データ
制御
データベース
20~
ビデオ
~24
記憶装置
~17

【図8】

Fig 8a

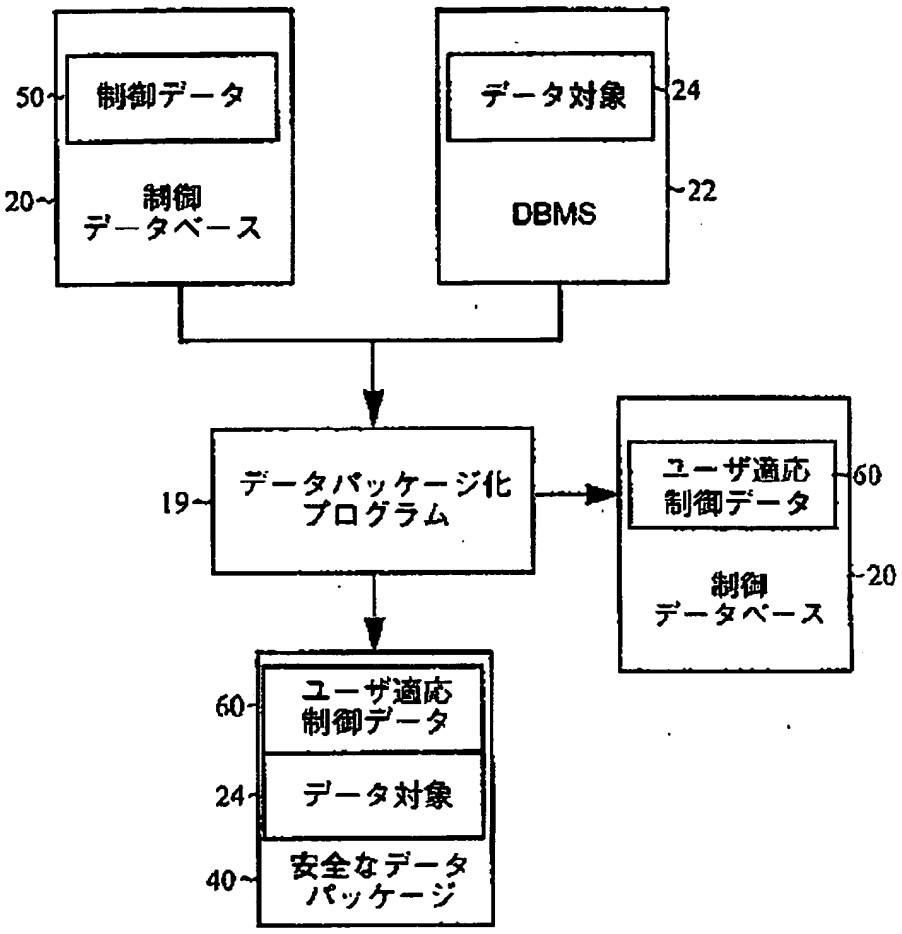
ヘッダ	対象識別子	123456789
	フォーマットコード	0010
	セキュリティコード	0010
	使用要素の数	2
	使用データのサイズ	17
	データ対象のサイズ	273
	第1の使用要素の識別子	001
	第1の使用要素のサイズ	6
	第1の使用要素のデータ	1
	第2の使用要素の識別子	002
	第2の使用要素のサイズ	3
	第2の使用要素のデータ	

Fig 8b

ヘッダ	対象識別子	123456790
	フォーマットコード	0010
	セキュリティコード	0010
	使用要素の数	2
	使用データのサイズ	17
	データ対象のサイズ	273
	第1の使用要素の識別子	001
	第1の使用要素のサイズ	6
	第1の使用要素のデータ	1
	第2の使用要素の識別子	002
	第2の使用要素のサイズ	3
	第2の使用要素のデータ	2

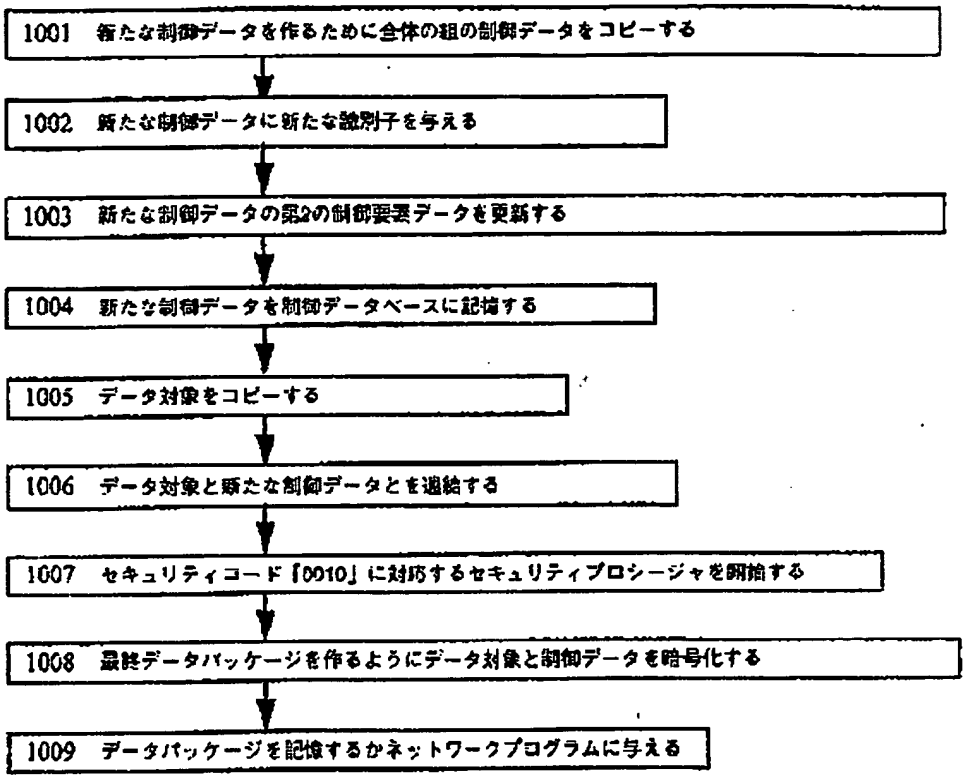
【図9】

Fig 9


50
制御データ
20
制御
データベース
データ対象
24
DBMS
22
19
データパッケージ化
プログラム
ユーザ適応
制御データ
60
制御
データベース
20
60
ユーザ適応
制御データ
24
データ対象
40
安全なデータ
パッケージ

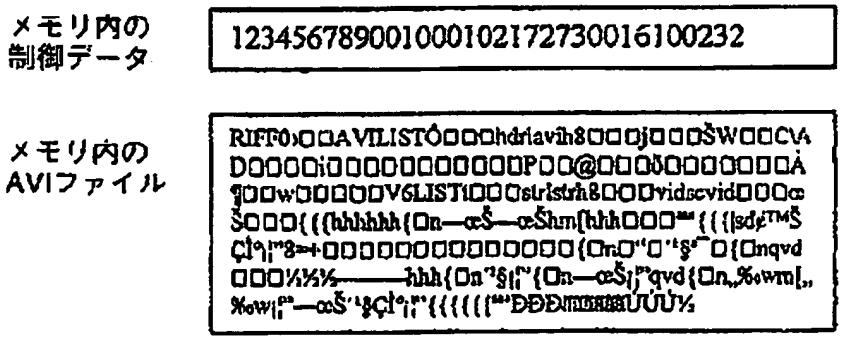
【図10】

Fig 10



【図11】

Fig 11



【図12】

Fig 12a

メモリ内の
連結された
制御データ
および
AVIファイル

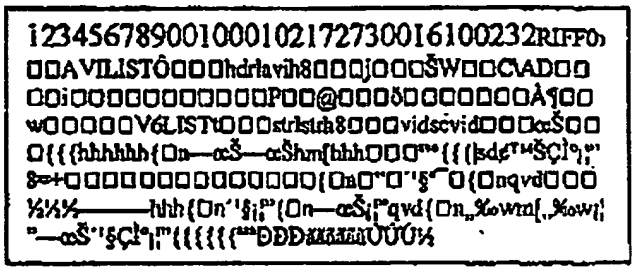
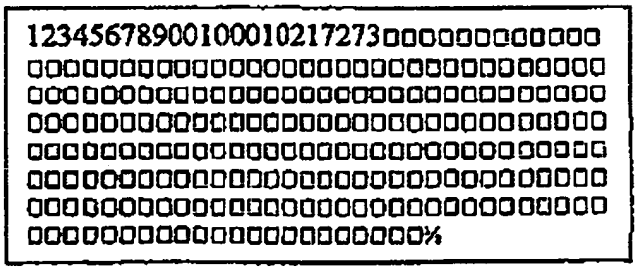


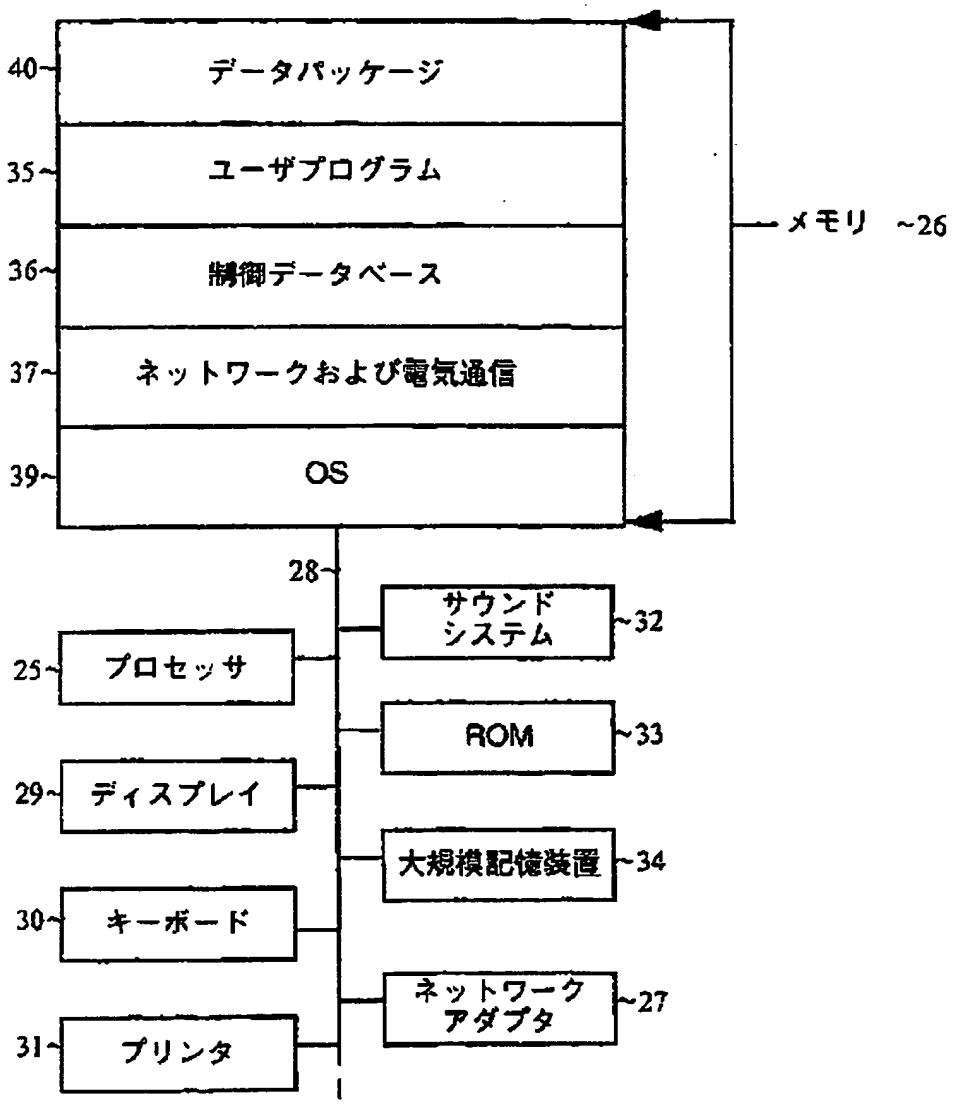
Fig 12b

メモリ内の
連結され
暗号化された
制御データ
および
AVIファイル



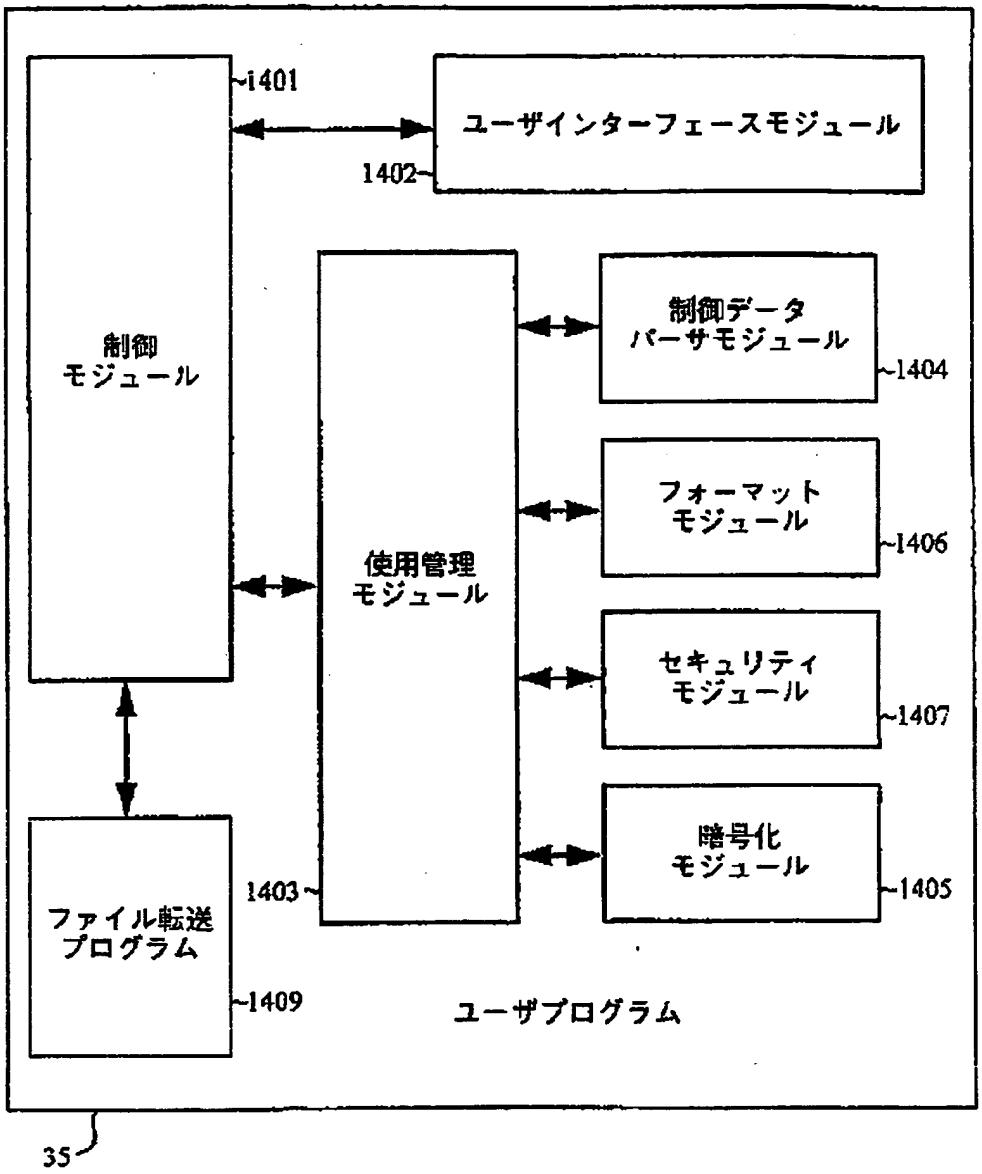
【図13】

Fig 13


40
データパッケージ
35
ユーザプログラム
36
制御データベース
37
ネットワークおよび電気通信
39
OS
メモリ ~26
28
サウンドシステム ~32
25
プロセッサ
ROM ~33
29
ディスプレイ
大規模記憶装置 ~34
30
キーボード
ネットワークアダプタ ~27
31
プリンタ

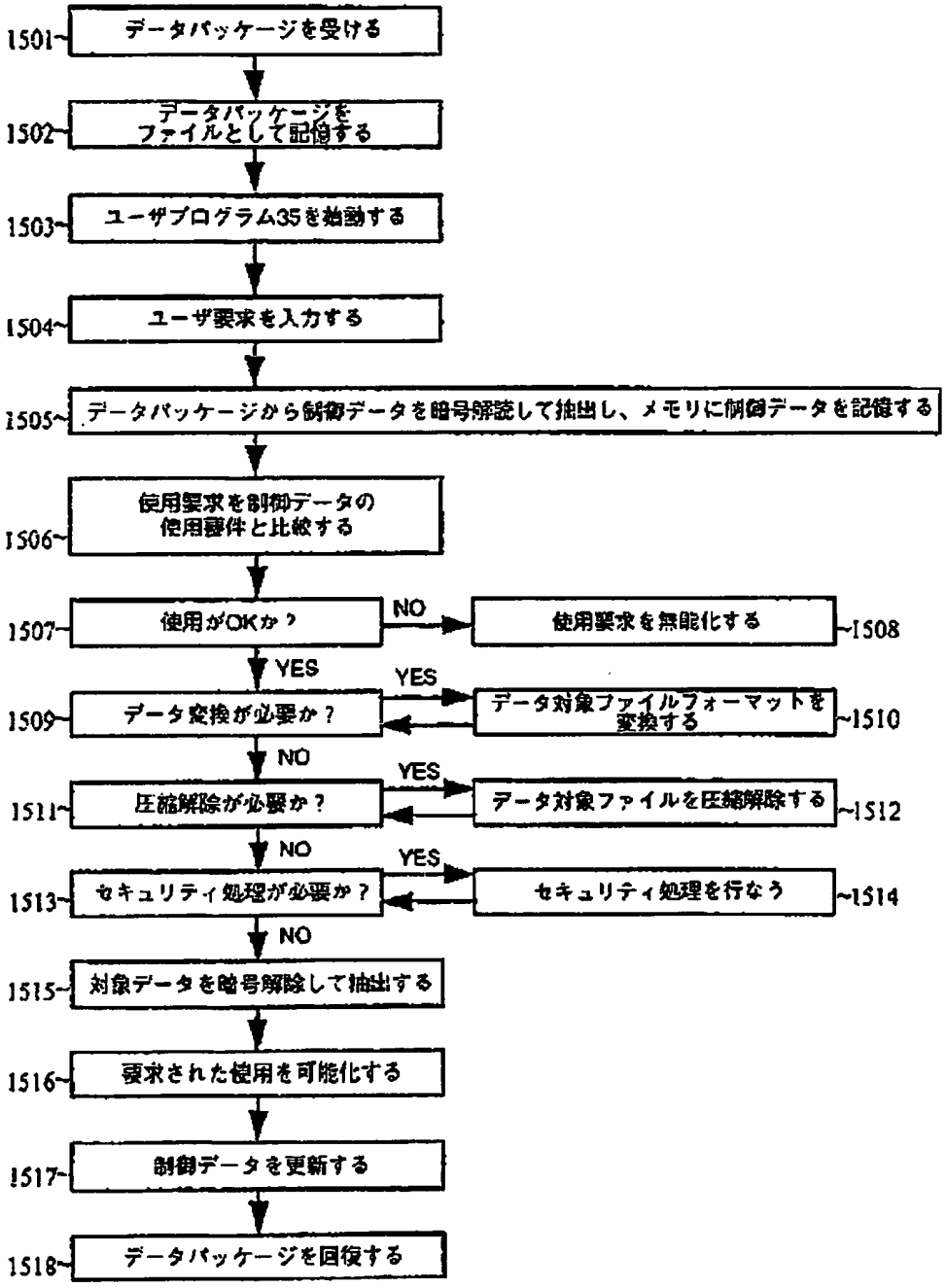
【図14】

Fig 14


1401
ユーザインターフェースモジュール
1402
制御
モジュール
使用管理
モジュール
制御データ
パーサモジュール
1404
フォーマット
モジュール
1406
セキュリティ
モジュール
1407
暗号化
モジュール
1405
1403
ファイル転送
プログラム
1409
ユーザプログラム
35

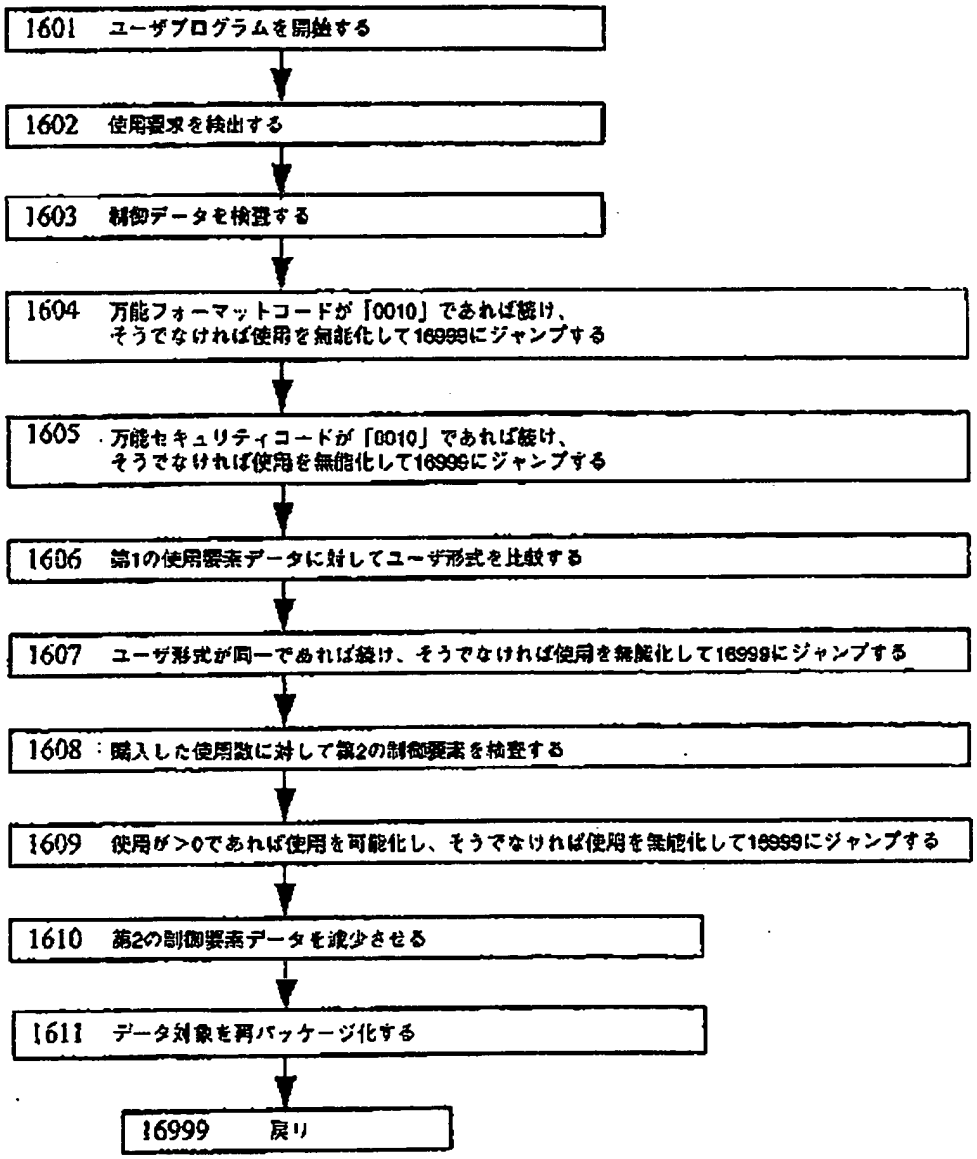
【図15】

Fig 15


1501 データパッケージを受ける
1502 データパッケージをファイルとして記憶する
1503 ユーザプログラム35を始動する
1504 ユーザ要求を入力する
1505 データパッケージから制御データを暗号解読して抽出し、メモリに制御データを記憶する
1506 使用要求を制御データの使用要件と比較する
1507 使用がOKか？
NO
1508 使用要求を無能化する
YES
1509 データ変換が必要か？
YES
1510 データ対象ファイルフォーマットを変換する
NO
1511 圧縮解除が必要か？
YES
1512 データ対象ファイルを圧縮解除する
NO
1513 セキュリティ処理が必要か？
YES
1514 セキュリティ処理を行なう
NO
1515 対象データを暗号解除して抽出する
1516 要求された使用を可能化する
1517 制御データを更新する
1518 データパッケージを回復する

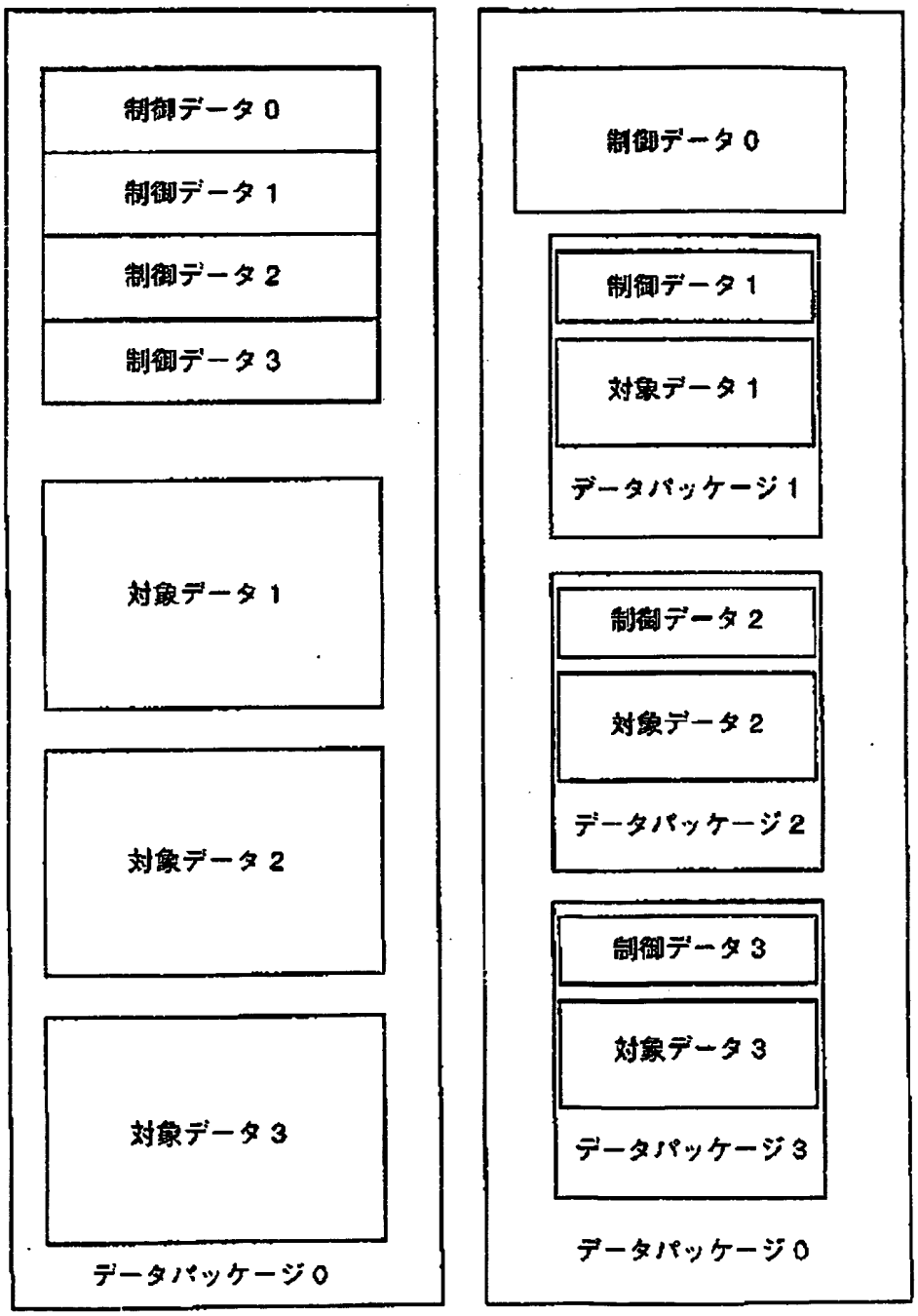
【図16】

Fig 16


1601 ユーザプログラムを開始する
1602 使用要求を検出する
1603 制御データを検査する
1604 万能フォーマットコードが「0010」であれば続け、
そうでなければ使用を無能化して16999にジャンプする
1605 万能セキュリティコードが「0010」であれば続け、
そうでなければ使用を無能化して16999にジャンプする
1606 第1の使用要素データに対してユーザ形式を比較する
1607 ユーザ形式が同一であれば続け、そうでなければ使用を無能化して16999にジャンプする
1608 購入した使用数に対して第2の制御要素を検査する
1609 使用が>0であれば使用を可能化し、そうでなければ使用を無能化して16999にジャンプする
1610 第2の制御要素データを減少させる
1611 データ対象を再パッケージ化する
16999 戻り

【図17】

Fig 17


制御データ0
制御データ1
制御データ2
制御データ3
対象データ1
対象データ2
対象データ3
データパッケージ0
制御データ0
制御データ1
対象データ1
データパッケージ1
制御データ2
対象データ2
データパッケージ2
制御データ3
対象データ3
データパッケージ3
データパッケージ0

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 96/00115

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: G06F 1/00, G06F 12/14
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5375240 A (GREGORY GRUNDY), 20 December 1994 (20.12.94), column 7, line 24 - column 10, line 46	1,2,7,13,14, 22
Y		16
A		6,8,10,23,24
	--	
X	EP 0367700 A2 (INTERNATIONAL BUSINESS MACHINES CORPORATION), 9 May 1990 (09.05.90), column 3, line 10 - column 6, line 59	1,22
Y		16
A		2,4,6,7,10, 13,14,25
	--	

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 August 1996	26 -08- 1996
Name and mailing address of the ISA Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Bo Gustavsson Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 96/00115

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5103476 A (DAVID P. WAITE ET AL), 7 April 1992 (07.04.92), claim 1	16,25
A		1,6-8,10,13, 14,22
X	US 5222134 A (DAVID P. WAITE ET AL), 22 June 1993 (22.06.93), column 3, line 43 - column 8, line 2	16,25
A		1,6-8,10,13, 14,22
A	US 5319705 A (BERNARD J. HALTER ET AL), 7 June 1994 (07.06.94), see whole document	1,2,6,7,10, 13,14,16,22, 23,25

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

31/07/96

International application No.
PCT/SE 96/00115

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A- 5375240	20/12/94	US-A- 5291598	01/03/94
EP-A2- 0367700	09/05/90	DE-D- 68926606	00/00/00
		JP-A- 2135938	24/05/90
		JP-B- 6048809	22/06/94
		US-A- 4953209	28/08/90
US-A- 5103476	07/04/92	CA-A- 2095723	08/05/92
		EP-A- 0556305	25/08/93
		JP-T- 6501120	27/01/94
		JP-B- 7089345	27/09/95
		US-A- 5222134	22/06/93
		WO-A- 9209160	29/05/92
US-A- 5222134	22/06/93	CA-A- 2095723	08/05/92
		EP-A- 0556305	25/08/93
		JP-T- 6501120	27/01/94
		JP-B- 7089345	27/09/95
		WO-A- 9209160	29/05/92
		US-A- 5103476	07/04/92
US-A- 5319705	07/06/94	JP-A- 7093148	07/04/95

フロントページの続き

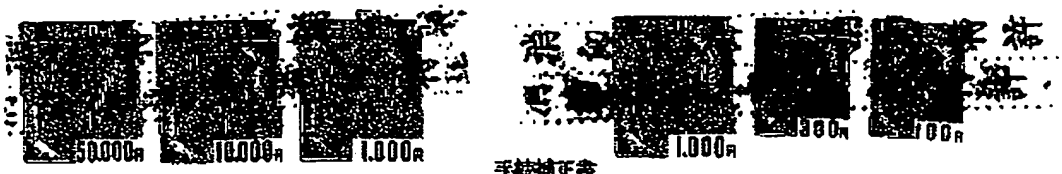
(51)Int.Cl.°	識別記号	FI	
		G06F 15/21	Z

(81)指定国　EP(AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(KE, LS, MW, SD, SZ, UG), UA(AZ, BY, KG, KZ, RU, TJ, TM), AL, AM, AT, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, CZ, DE, DE, DK, DK, EE, EE, ES, FI, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成17年3月10日(2005.3.10)

【公表番号】特表平10-513289
【公表日】平成10年12月15日(1998.12.15)
【出願番号】特願平8-523476
【国際特許分類第７版】
Ｇ０６Ｆ　17/60
Ｇ０６Ｆ　 9/06
Ｇ０６Ｆ　15/00
Ｇ０９Ｃ　 1/00
【ＦＩ】
Ｇ０６Ｆ　15/21　３３０
Ｇ０６Ｆ　 9/06　５５０Ａ
Ｇ０６Ｆ　 9/06　５５０Ｚ
Ｇ０６Ｆ　15/00　３３０Ｚ
Ｇ０９Ｃ　 1/00　６６０Ｄ
Ｇ０６Ｆ　15/21　Ｚ

【手続補正書】
【提出日】平成16年7月7日(2004.7.7)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】補正の内容のとおり
【補正方法】変更
【補正の内容】



手続補正書

平成１６年７月７日

(62,400円)

特許庁長官 小川 洋 殿

1．事件の表示

平成８年特許願第５２３４７６号

2．補正をする者

住所（居所）アメリカ合衆国 カリフォルニア、サンタ クララ、
デ ラ クルズ ブールバード ２８３０

氏名（名称）マクロビジョン コーポレイション

3．代理人

住所 〒150-6032 東京都渋谷区恵比寿４丁目２０番３号
恵比寿ガーデンプレイスタワー３２階

氏名 (7015) 弁理士 伊 東 忠 彦

電話０３(５４２４)２５１１番(代表)

4．補正により増加する請求項の数 ３９

5．補正対象書類名

請求の範囲

6．補正対象項目名

請求の範囲

7．補正の内容

請求の範囲の記載を別紙のとおり補正する。

請求の範囲

1．データ対象の使用法についての制御条件に従うようにデータ対象を管理する方法であって、
データ対象供給者のデータプロセッサによりアクセス可能となるようにデータ対象をメモリ装置に記憶し、
該データ対象の使用法について可変な数の制御条件を設け、
上記データプロセッサによって、該可変な数の制御条件に従った該データ対象の使用法を定める少なくとも１つ又は複数の使用法制御要素を含んだ制御データの全体セットを、使用法についての該可変な数の制御条件に基づいて該データ対象に対して設け、
上記データプロセッサによってアクセス可能となるように該制御データの全体セットをメモリ装置に記憶し、
該制御データの全体セットを該データ対象のコピーと連結し、
少なくとも該データ対象のコピーと上記１つ又は複数の使用法制御要素を暗号化してユーザへの転送準備が整った安全なデータパッケージを生成する、
各ステップを含む方法。
2．請求の範囲第１項記載の方法において、暗号化するステップはデータ対象および制御データの全体セットを暗号化することを含む方法。
3．請求の範囲第１項あるいは第２項記載の方法において、制御データを設けるステップは制御データの全体セットを一意に識別する識別子を設けることを含む方法。
4．請求の範囲第１項、第２項あるいは第３項記載の方法において、制御データの全体セットを設けるステップは、データ対象の使用を許す前に適用すべきセキュリティプロセスを識別するセキュリティ制御要素を設けることを含む方法。
5．請求の範囲の上述の項のうちの任意の１項記載の方法において、制御データの全体セットを設けるステップは制御データのフォーマットを識別するフォーマット制御要素を設けるステップを含む方法。
6．請求の範囲の上述の項のうちの任意の１項記載の方法であって、
ユーザによるデータ対象の使用許可についての要求に応じて、上記使用法制御要素の少なくとも１つを含む制御データの全体セットの少なくともサブセットからなる制御データのユーザセットを設け、
上記連結するステップにおいて、上記制御データの全体セットの代わりに該制御データのユーザセットを使用し、

上記暗号化するステップにおいて、上記制御データの全体セットの上記１つ又は複数の使用法制御要素の代わりに上記制御データのユーザセットの上記少なくとも１つの使用法制御要素を使用し、

ユーザへの上記データパッケージの転送を許可する前に、データ対象の使用許可の上記要求が承諾されたことをチェックする

各ステップを更に含む方法。

７．請求の範囲の上述の項のうちの任意の１項記載の方法であって、上記データプロセッサにおいてユーザによる使用許可のための要求を受け、許可が要求される使用法を上記制御データの全体セットの上記１つ又は複数の使用法制御要素と比較し、許可が要求される使用法が上記少なくとも１つ又は複数の使用法制御要素によって定められる使用法に従う場合に許可を承諾する

各ステップを更に含む方法。

８．請求の範囲第７項記載の方法において、許可を承諾する前に、要求された使用許可のための支払いを確実化するステップを更に含む方法。

９．請求の範囲第６－８項のうちの任意の１項記載の方法において、データ対象は少なくとも２つの構成要素データ対象からなり、上記制御データのユーザセットは、ユーザによる上記構成要素データ対象の１つの使用に対する許可の要求に応じて、その構成要素データ対象に対してだけに作られてこの構成要素データ対象のコピーとだけに連結されることを特徴とする方法。

10．請求の範囲第６－９項のうちの任意の１項記載の方法において、上記データ供給者のデータプロセッサはデータネットワークに接続され、上記許可の要求は同様に該データネットワークに接続された上記ユーザのデータプロセッサから受信され、上記データパッケージを該データネットワークを介して該ユーザのデータプロセッサに転送するステップを更に含む方法。

11．請求の範囲第６－８項あるいは第１０項のうちの任意の１項記載の方法において、データ対象は少なくとも２つの構成要素データ対象を含んだ複合データ対象であり、制御データの全体セットを設けるステップは複合データ対象のそれぞれおよび複合データ対象に対するそれぞれの制御データの全体セットを設けるステップからなり、制御データのユーザセットを設けるステップは構成要素データ対象のそれぞれおよび複合データ対象に対するそれぞれの制御データのユーザセットを設けるステップを更に含む方法。

12．請求の範囲の上述の項のうちの任意の１項記載の方法において、制御データの上記ユーザセットのコピーを上記データ対象供給者のプロセッサに記憶するステップを更に含む方法。

13．請求の範囲の上述の項のうちの任意の１項記載の方法であって、

ユーザのデータプロセッサにおいて上記データパッケージを受け取り、

該ユーザのデータプロセッサによりアクセス可能となるようにメモリ装置に該データパッケージを記憶し、

上記１つ又は複数の使用法制御要素を暗号解除し、

データ対象の使用についてのユーザによる要求に応じて、要求された使用が上記制御データの全体セットの少なくとも１つの使用法制御要素によって規定された使用法に従うかどうかをチェックし、

該制御データの全体セットの該少なくとも１つの使用法制御要素によって規定される使用法に該要求された使用法が従う場合にデータ対象を暗号解除すると共に該要求された使用を可能にし、そうでない場合に該要求された使用を不可能にする

各ステップを更に含む方法。

14. 請求の範囲第６－１２項のうちの任意の１項記載の方法であって、

ユーザのデータプロセッサにおいて該データパッケージを受け取り、

該ユーザのデータプロセッサによりアクセス可能となるようにメモリ装置に該データパッケージを記憶し、

上記制御データのユーザセットの上記少なくとも１つの使用法制御要素を暗号解除し、

データ対象の使用についてのユーザによる要求に応じて、該要求された使用が該制御データのユーザセットの該少なくとも１つの使用制御要素によって規定された使用法に従うかどうかをチェックし、

該制御データのユーザセットの該少なくとも１つの使用法制御要素によって規定される使用法に該要求された使用法が従う場合にデータ対象を暗号解除すると共に該要求された使用を可能にし、そうでない場合に該要求された使用を不可能にする

各ステップを更に含む方法。

15. 請求の範囲第１３項あるいは第１４項記載の方法であって、上記データ対象の使用の後に、該データ対象および上記１つ又は複数の使用法制御要素を再連結し、少なくとも該データ対象および該１つ又は複数の使用法制御要素を再暗号化し、このようにして再パッケージ化したデータパッケージを上記ユーザのデータプロセッサのメモリに記憶する各ステップを更に含む方法。

16. データ対象の使用法についての制御条件に従うように該データ対象のユーザによる使用を制御するための方法であって、

該データ対象の使用法について可変な数の制御条件を設け、

該可変な数の制御条件に従った該データ対象の使用法を定める暗号化された少なくとも１つの使用法制御要素を含む制御データと、暗号化された該データ対象とを含むデータパッケージを、該ユーザのデータプロセッサによりアクセ

ス可能となるようにメモリ装置に記憶し、
該データ対象の使用についての該ユーザによる要求を受け、
該制御データを暗号解除し、
該データ対象の使用についての該ユーザによる該要求に応じて、該要求された使用が上記制御データの少なくとも１つの使用法制御要素によって規定された使用法に従うかどうかをチェックし、
該制御データの該少なくとも１つの使用法制御要素によって規定される該使用法に該要求された使用が従う場合に該データ対象を暗号解除して該要求された使用を可能にし、それ以外の場合に該要求された使用を不可能にする
各ステップを含む方法。
17. 請求の範囲第１６項記載の方法において、使用法制御要素は該データ対象の使用の後に更新されるようにした方法。
18. 請求の範囲第１６項あるいは第１７項記載の方法において、上記制御データは上記少なくとも１つの使用法制御要素に従ってユーザがデータ対象を使用することを許可される回数の指示からなり、データ対象の要求された使用は上記回数が１あるいはそれ以上の時にのみ可能化され、上記回数は要求された使用が可能化される時に１だけ減少されるようにした方法。
19. 請求の範囲第１６－１８項のうちの任意の１項記載の方法において、制御データはセキュリティ制御要素を備え、更に、データ対象の各使用の前にセキュリティ制御要素において定められたセキュリティプロシージャを実行するステップを具備した方法。
20. 請求の範囲第１６－１９項のうちの任意の１項記載の方法であって、要求された使用が少なくとも１つの使用法制御要素によって規定された使用法に従うかどうかをチェックするステップは、ユーザのデータプロセッサが制御データのセキュリティ制御要素で特定されたセキュリティプロシージャを実行することが可能であるかをチェックし、可能でない場合には該使用を不可能にするステップを含む方法。
21. 請求の範囲第１６－２０項のうちの任意の１項記載の方法において、データ対象の使用の後に、データ対象および１つ又は複数の使用制御要素を再連結すること、少なくともデータ対象および１つ又は複数の使用制御要素を再暗号化すること、このようにした再パッケージ化されたデータパッケージをユーザのデータプロセッサのメモリに記憶すること、のステップを更に具備した方法。
22. データ対象の使用法についての制御条件に従うようにデータ対象を管理するシステムであって、
可変な数の制御条件を設ける手段と、
データ対象供給者のデータプロセッサに設けられ、該可変な数の制御条件に

従った該データ対象の使用法を定める少なくとも１つ又は複数の使用法制御要素を含む制御データの全体セットを、使用法についての該可変な数の制御条件に基づいて該データ対象に対して設ける第１の手段と、

上記データプロセッサによりアクセス可能であり、該データ対象と該制御データの全体セットを記憶するための記憶手段と、

該制御データの全体セットを該データ対象のコピーと連結するための連結手段と、

該データ対象の該コピーと少なくとも上記１つ又は複数の使用法制御要素とを暗号化して、ユーザへの転送準備が整った安全なデータパッケージを作る暗号化手段と、

を含むシステム。

23. 請求の範囲第２２項記載のシステムであって、

上記データプロセッサに設けられ、ユーザによるデータ対象の使用許可の要求に応じて、上記使用制御要素の少なくとも１つからなる制御データの全体セットのサブセットから少なくとも構成される制御データのユーザセットを作る第２の手段と、

上記データプロセッサに設けられ、該データ対象の使用許可のための上記要求が該ユーザへの該データパッケージの転送を許可する前に承諾されたことをチェックするチェック手段と、を更に具備したシステム。

24. 請求の範囲第２２項あるいは第２３項記載のシステムであって、該制御データの全体セットは、該ユーザが該データ対象を更に配布する権利を定めた制御データ要素を含むシステム。

25. データ対象の使用法についての制御条件に従うようにデータ対象のユーザによる使用を制御するためのシステムであって、

可変な数の制御条件を設ける手段と、

該可変な数の制御条件に従った該データ対象の使用法を定める少なくとも１つの使用法制御要素を含む制御データとデータ対象とを含むデータパッケージを格納する格納手段と、

上記少なくとも１つの使用法制御要素および該データ対象を暗号解除する手段と、

ユーザにより要求された使用が上記少なくとも１つの使用制御要素によって定められる使用法に従うかどうかをチェックするためのチェック手段と、

該使用が上記少なくとも１つの使用法制御要素によって定められた使用法に従う時に上記ユーザによって要求された使用を可能にするための可能化手段と、

該使用が上記少なくとも１つの使用法制御要素によって定められた使用法に従わない時に上記ユーザによって要求された使用を不可能にするための不能化

手段と、
を含むシステム。
26. 請求の範囲第２５項記載のシステムであって、上記データ対象の使用後に該データ対象を再パッケージ化するための手段を更に含むシステム。
27. 請求項１６記載の方法であって、
該可変な数の制御条件に従った該データ対象の使用法を定める暗号化された少なくとも１つの使用法制御要素を含む制御データのユーザセットと、暗号化されたデータ対象とを各々が含む少なくとも２つのデータパッケージを、該ユーザのデータプロセッサによりアクセス可能となるようにメモリ装置に記憶し、
該制御データのユーザセットの該使用法制御要素を暗号解除し、
一致を見出すために上記少なくとも２つのデータパッケージの上記使用法制御要素を検査し、
一致が見い出されると、上記制御データのユーザセットにおいて特定される行為を上記データプロセッサを用いて実行する、
各ステップを更に含む方法。
28. 請求の範囲第２７項記載の方法であって、各データパッケージの少なくとも１つの使用法制御要素を更新し、上記データ対象の使用の後に、該データ対象のそれぞれとその少なくとも１つの使用法制御要素とを連結し、連結されたデータ対象のそれぞれとその少なくとも１つの使用法制御要素とを再暗号化し、該再パッケージ化したデータ対象をそれぞれの提供者に転送する各ステップを更に含む方法。
29. データ対象の使用法についての制御条件に従うようにデータ対象を管理する方法であって、
データ対象の使用法について可変な数の制御条件を設け、
該可変な数の制御条件に従った該データ対象の使用法を定める少なくとも１つ又は複数の使用法制御要素を含んだ制御データの全体セットを、使用法についての該可変な数の制御条件に基づいて該データ対象に対して設け、
少なくとも該データ対象を暗号化してユーザデータプロセッサへの転送準備が整った安全なデータパッケージを生成する
段階を含む方法。
30. 該データ対象と該制御データの全体セットとを一緒に暗号化する段階を更に含む請求項２９記載の方法。
31. 該制御データの全体セットを設ける段階は、該制御データの全体セットを一意に識別する識別子を設ける段階を含む請求項２９記載の方法。
32. 該制御データの全体セットを設ける段階は、該データ対象の使用を許す前に適用すべきセキュリティプロセスを識別するセキュリティ制御要素を設ける

段階を含む請求項２９記載の方法。
33. 該制御データの全体セットを設ける段階は該制御データのフォーマットを識別するフォーマット制御要素を設ける段階を含む請求項２９記載の方法。
34. 使用許可についてユーザリクエストを受け取り、
許可がリクエストされた使用法と該制御データの全体セットの該１つ又は複数の使用法制御要素とを比較し、
許可がリクエストされた該使用法が該１つ又は複数の使用法制御要素により定められる使用法に従う場合に該許可を与える
段階を更に含む請求項２９記載の方法。
35. 該許可を与える前に、該リクエストされた使用許可についての支払いを要求する段階を更に含む請求項３４記載の方法。
36. 該安全なデータパッケージを該データプロセッサに送信し、
該データ対象の使用についてのユーザリクエストに応答して、該リクエストされた使用法が該制御データの全体セットの該少なくとも１つの使用法制御要素により定められる使用法に従うか否かをチェックし、
該リクエストされた使用法が該制御データの全体セットの該少なくとも１つの使用法制御要素により定められる使用法に従う場合に該データ対象を解読して該リクエストされた使用を可能にする
段階を更に含む請求項２９記載の方法。
37. 該データ対象の該使用の後に、該データ対象と該１つ又は複数の使用法制御要素とを結合し、
少なくとも該データ対象を再暗号化する
段階を更に含む請求項３６記載の方法。
38. データ対象の使用法についての制御条件に従うように該データ対象のユーザによる使用を制御する方法であって、
該データ対象の使用法について可変な数の制御条件を設け、
該可変な数の制御条件に従った該データ対象の使用法を定める少なくとも１つの使用法制御要素を含んだ制御データと、暗号化されたデータ対象とを設け、
該データ対象の使用についてのユーザリクエストを受け取り、
該データ対象の使用についての該ユーザリクエストに応答して、該リクエストされた使用法が該制御データの該少なくとも１つの使用法制御要素により定められる使用法に従うか否かをチェックし、
該リクエストされた使用法が該制御データの該少なくとも１つの使用法制御要素により定められる該使用法に従う場合に該データ対象を解読して該リクエストされた使用を可能にする
段階を含む方法。

段階を含む請求項２９記載の方法。
33. 該制御データの全体セットを設ける段階は該制御データのフォーマットを識別するフォーマット制御要素を設ける段階を含む請求項２９記載の方法。
34. 使用許可についてユーザリクエストを受け取り、
許可がリクエストされた使用法と該制御データの全体セットの該１つ又は複数の使用法制御要素とを比較し、
許可がリクエストされた該使用法が該１つ又は複数の使用法制御要素により定められる使用法に従う場合に該許可を与える
段階を更に含む請求項２９記載の方法。
35. 該許可を与える前に、該リクエストされた使用許可についての支払いを要求する段階を更に含む請求項３４記載の方法。
36. 該安全なデータパッケージを該データプロセッサに送信し、
該データ対象の使用についてのユーザリクエストに応答して、該リクエストされた使用法が該制御データの全体セットの該少なくとも１つの使用法制御要素により定められる使用法に従うか否かをチェックし、
該リクエストされた使用法が該制御データの全体セットの該少なくとも１つの使用法制御要素により定められる使用法に従う場合に該データ対象を解読して該リクエストされた使用を可能にする
段階を更に含む請求項２９記載の方法。
37. 該データ対象の該使用の後に、該データ対象と該１つ又は複数の使用法制御要素とを結合し、
少なくとも該データ対象を再暗号化する
段階を更に含む請求項３６記載の方法。
38. データ対象の使用法についての制御条件に従うように該データ対象のユーザによる使用を制御する方法であって、
該データ対象の使用法について可変な数の制御条件を設け、
該可変な数の制御条件に従った該データ対象の使用法を定める少なくとも１つの使用法制御要素を含んだ制御データと、暗号化されたデータ対象とを設け、
該データ対象の使用についてのユーザリクエストを受け取り、
該データ対象の使用についての該ユーザリクエストに応答して、該リクエストされた使用法が該制御データの該少なくとも１つの使用法制御要素により定められる使用法に従うか否かをチェックし、
該リクエストされた使用法が該制御データの該少なくとも１つの使用法制御要素により定められる該使用法に従う場合に該データ対象を解読して該リクエストされた使用を可能にする
段階を含む方法。

39. 該使用法制御要素は、該データ対象の少なくとも一回の使用の後に更新される請求項３８記載の方法。
40. 該制御データは、該少なくとも１つの使用法制御要素に従って該データ対象を使用することの許可を該ユーザが与えられた回数を示す指示を含み、該回数が１又はそれ以上のときにのみ該データ対象の該リクエストされた使用は可能とされ、該リクエストされた使用が可能とされると該回数は１だけ減少される請求項３８記載の方法。
41. 該制御データはセキュリティ制御要素を含み、該データ対象の各使用の前に該セキュリティ制御要素に定められたセキュリティプロシージャを実行する段階を更に含む請求項３８記載の方法。
42. 該リクエストされた使用が該少なくとも１つの使用法制御要素によって定められる使用法に従うか否かをチェックする段階は、データプロセッサが該少なくとも１つの使用法制御要素のセキュリティ制御要素で特定されたセキュリティプロシージャを実行することが可能であるかをチェックし、可能でない場合には該使用を不可能にする段階を含む方法。
43. 該データ対象の該使用の後に、該データ対象及び該１つ又は複数の使用制御要素を結合し、少なくとも該データ対象を再暗号化する段階を更に含む請求項３８記載の方法。
44. データ対象の使用法についての制御条件に従うようにデータ対象を管理するシステムであって、
可変な数の制御条件を受け取るユーザインタフェースモジュールと、
該可変な数の制御条件に従った該データ対象の使用法を定める少なくとも１つ又は複数の使用法制御要素を含んだ制御データの全体セットを、使用法についての該可変な数の制御条件に基づいて該データ対象に対して設けると共に、制御データの該全体セットをパッケージ化するパッケージ化モジュールと、
該データ対象を暗号化してユーザへの転送準備が整った安全なデータパッケージを生成する暗号化モジュール
を含むシステム。
45. 制御データの該全体セットは該データ対象の更なる配布を制御する制御データ要素を含む請求項４４記載のシステム。
46. 該使用法制御要素の１つはセキュリティー手順を定めるセキュリティー制御要素を含む請求項４４記載のシステム。
47. データ対象の使用法についての制御条件に従うように該データ対象のユーザによる使用を制御するシステムであって、
可変な数の制御条件を受け取り、該可変な数の制御条件に従った少なくとも１つの使用法制御要素により定められる使用法に、該ユーザによりリクエスト

された使用が従うか否かをチェックし、該使用が該少なくとも１つの使用法制御要素により定められる該使用法に従わない場合に該ユーザによりリクエストされた該使用を不可能にする使用管理モジュールと
リクエストされた使用の該使用管理モジュールによるチェックに応答して、該データ対象を解読する解読モジュール
を含むシステム。
48．該使用法制御要素の１つはセキュリティー手順を定めるセキュリティー制御要素を含む請求項４７記載のシステム。
49．該セキュリティー手順はＲＳＡ暗号化アルゴリズムである請求項４８記載のシステム。
50．該使用管理モジュールは使用後に該データ対象を暗号化する請求項４７記載のシステム。
51．データ対象の使用法についての可変な数の条件に従ってユーザによるデータ対象の使用を制御する方法であって、
該可変な数の条件に従った該データ対象の使用法を定める少なくとも１つの使用法制御要素を含む制御データのユーザセットと、暗号化されたデータ対象とを各々が含む少なくとも２つのデータパッケージを提供し、
一致を見出すために該少なくとも２つのデータパッケージの該使用法制御要素を検査し、
該少なくとも２つのデータパッケージの制御データの該ユーザセットにおいて特定される行為を実行する、
各段階を含む方法。
52．該少なくとも２つのデータパッケージの１つは売り注文であり、該少なくとも２つのデータパッケージの１つは買い注文である請求項５１記載の方法。
53．データプロセッサが該少なくとも１つの使用法制御要素のセキュリティー制御要素で特定されたセキュリティー手順を実行することが可能であるか否かをチェックし、該データプロセッサが該セキュリティー手順を実行し該データ対象を解読することが可能でない場合には該使用を不可能にする段階を更に含む方法。
54．各データパッケージの該少なくとも１つの使用法制御要素を更新し、
該データ対象の各々を再暗号化する
段階を更に含む請求項５３記載の方法。
55．データ対象の使用法についての可変な数の制御条件に従うようにデータ対象を管理する方法であって、
該データ対象の使用法について可変な制御条件を設け、
該可変な制御条件に従った該データ対象の使用法を定める少なくとも１つ又

は複数の使用法制御要素を含んだ制御データの全体セットを、使用法についての譲可変な制御条件に基づいて該データ対象に対して設け、
制御データの該全体セットの少なくともサブセットを含み、該使用法制御要素の少なくとも１つを含む制御データのユーザセットを、該データ対象の使用許可についてのユーザからのリクエストに応答して提供し、
少なくとも該データ対象を暗号化して安全なデータパッケージを生成し、
該データパッケージの該ユーザへの転送を許可する前に、該データ対象の使用許可についての該リクエストが承諾されたことをチェックする
各段階を含む方法。
56. データプロセッサが該少なくとも１つの使用法制御要素のセキュリティー制御要素で特定されたセキュリティー手順を実行することが可能であるか否かをチェックし、該データプロセッサが該セキュリティー手順を実行することが可能でない場合に該使用を不可能にする段階を更に含む請求項５５記載の方法。
57. 該データ対象は少なくとも２つの構成要素データ対象を含み、該構成要素データ対象の１つについてのユーザからの使用許可のリクエストに応答して、該１つの構成要素データ対象についてのみ制御データの該ユーザセットが生成され、該構成要素データ対象のコピーとのみ結合される請求項５５記載の方法。
58. 該許可リクエストはユーザからデータネットワークを介して受信される請求項５５記載の方法。
59. 該データ対象は少なくとも２つの構成要素データ対象を含む複合データ対象であり、制御データの全体セットを提供する段階は、該構成要素データ対象と該複合データ対象の各々について制御データのそれぞれの全体セットを提供する段階を含み、制御データのユーザセットを提供する段階は、該構成要素データ対象と該複合データ対象の各々について制御データのそれぞれのユーザセットを提供する段階を含む請求項５５記載の方法。
60. データ対象提供者のプロセッサに制御データの該ユーザセットを格納する段階を更に含む請求項５５記載の方法。
61. 該データパッケージを送信し、
該データ対象の使用についての該ユーザからのリクエストに応答して、制御データの該ユーザセットの該少なくとも１つの使用法制御要素により定められる該使用法に該リクエストされた使用が従うか否かをチェックし、
制御データの該ユーザセットの該少なくとも１つの使用法制御要素により定められる該使用法に該リクエストされた使用が従う場合に、該データ対象を解読し該リクエストされた使用を可能にする
段階を更に含む請求項５５記載の方法。
62. 該データパッケージを送信し、

該データ対象を再暗号化する
段階を更に含む請求項５５記載の方法。
63. データ対象の使用法についての制御条件に従うようにデータ対象を管理するシステムであって、
可変な条件に従ったデータ対象の使用法を定める少なくとも１つ又は複数の使用法制御要素を含んだ制御データの全体セットを、使用法についての該可変な条件に基づいて該データ対象に対して設け、制御データの該ユーザセットと該データ対象とを結合し、制御データの該全体セットの少なくともサブセットであり該使用法制御要素の少なくとも１つを含むサブセットを含む制御データのユーザセットを、該データ対象の使用許可についてのユーザからのリクエストに応答して提供するパッケージ化モジュールと、
該データ対象を暗号化して、ユーザへの転送準備が整った安全なデータパッケージを生成する暗号化モジュールと、
該データパッケージの該ユーザへの転送を許可する前に、該データ対象の使用許可についての該リクエストが承諾されたことをチェックする制御モジュール
を含むシステム。
64. データ対象の使用法についての制御条件に従うようにデータ対象を管理する方法であって、
データ対象提供者のプロセッサのメモリにデータ対象を格納し、
該データ対象の使用法について可変な数の制御条件を設け、
該可変な数の制御条件に従った該データ対象の使用法を定める少なくとも１つ又は複数の使用法制御要素を含んだ制御データのセットを、使用法についての該可変な数の制御条件に基づいて該データ対象に対して設ける
段階を含む方法。
65. 該データ対象と該制御データのセットとをデータプロセッサに送信し、
該データ対象の使用についてのユーザからのリクエストに応答して、該制御データのセットの該少なくとも１つの使用法制御要素により定められる使用法に該リクエストされた使用が従うか否かをチェックし、
該制御データのセットの該少なくとも１つの使用法制御要素により定められる該使用法に従って該リクエストされた使用を可能にする
段階を更に含む請求項６４記載の方法。
66. 該データ対象の該使用の後に、該データ対象と該１つ又は複数の使用法制御要素とを結合する段階を更に含む請求項６４記載の方法。
67. 該データ要素はデジタルデータである請求項６４記載の方法。

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.